UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

A Comparative Study of Interdisciplinary Cybersecurity Education

LISA HO, SAHAR RABIEI, DRAKE WHITE

LISA HO **Project Lead**

Academic Director - Masters in Information and Cybersecurity, UC Berkeley

SAHAR RABIEI **Lead Researcher**

Masters Student - Cybersecurity and Information, UC Berkeley

DRAKE WHITE **Researcher**

Masters Student - Information Management and Systems, UC Berkeley

https://cltc.berkeley.edu/publication/interdisciplinary-cybersecurity-education

CLTC WHITE PAPER SERIES

A Comparative Study of Interdisciplinary Cybersecurity Education

UNIVERSITY OF CALIFORNIA, BERKELEY,
CENTER FOR LONG-TERM CYBERSECURITY *and* SCHOOL OF INFORMATION
for the WILLIAM + FLORA HEWLETT FOUNDATION

WILLIAM + FLORA
Hewlett Foundation

LISA HO, SAHAR RABIEI, DRAKE WHITE

September 2023

CLTC
Center for Long-Term
Cybersecurity
UC Berkeley

Contents

EXECUTIVE SUMMARY 1

I. INTRODUCTION 3

Description and Purpose 3

Definitions, Methodology, and Scope 4

Limitations 8

II. OBSERVATIONS AND ANALYSIS 9

Overview 9

Academic Discipline and Interdisciplinary Focus 10

Cybersecurity-Specific, Cyber-Related, and Not-Cybersecurity Course Offerings 15

Programming Requirements 16

- Programming Bridge Courses 18

Capstone, Practicum, and Clinical Course Offerings 19

- Clinics 19
- Practicums 19
- Capstones 20
- Other 20

Cybersecurity Curriculum Framing 20

- Distribution of Curriculum Topics 21

Policy Topics 22

III. RECOMMENDATIONS 26

Curriculum Recommendations 26

- Build Pathways for Diversity of Background and Thought 26
- Balance Foundational and Current Topics 27
- Incorporate Global Scope 27

Advocacy Recommendations 28

- Enhance and Infuse Policy into Cybersecurity Frameworks 28
- Seek Recognition of Interdisciplinary Programs 29

IV. CONCLUSION 30

V. APPENDICES 31

A. Focus Group Feedback 31

Curriculum Technical Balance 31

Curriculum Drivers 34

Curriculum Currency and Future Directions 35

B. Policy Course Offerings 36

C. Syllabi 42

D. Primary and Secondary Course Topics by Program 44

E. NICE Framework Specialty Areas and Work Roles 53

SECURELY PROVISION (SP) 54

OPERATE and MAINTAIN (OM) 54

OVERSEE and GOVERN (OV) 54

PROTECT and DEFEND (PR) 54

ANALYZE (AN) 55

COLLECT and OPERATE (CO) 55

INVESTIGATE (IN) 55

F. CSEC2017 Joint Task Force Cybersecurity Curricula 56

Data Security 56

Software Security 56

Component Security 56

Connection Security 56

System Security 57

Human Security 57

Organizational Security 57

Societal Security 57

Policy Topics within CSEC2017 Knowledge Areas 58

VI. ACKNOWLEDGMENTS 60

ABOUT THE AUTHORS 61

Executive Summary

Since 2014, the William and Flora Hewlett Foundation Cyber Initiative has allocated grants to support interdisciplinary cybersecurity education at universities across the United States, as part of a broader goal to develop a field of cyber policy experts and institutions that can "anticipate, analyze, and address [cybersecurity] risks thoughtfully and systematically."[1] This paper presents a comparative study of the interdisciplinary cybersecurity education landscape to guide educational institutions in developing and creating cybersecurity programs. We compiled publicly available information about a selection of 17 interdisciplinary cybersecurity degree programs, with a focus on masters programs offered by Hewlett grantees. We then supplemented our data collection with two focus group meetings with representatives from the programs studied, as well as from recent Hewlett grantees.[2]

Programs in the study depicted a range of models for interdisciplinary cybersecurity education and a variety of approaches for cultivating diverse and interdisciplinary thinking in the field. These models include dual-degree programs and curriculum requirements that span multiple schools and disciplines, and that are designed to foster cross-disciplinary thinking and develop student competency in both technical and policy-oriented domains.

The study revealed a variety of important insights for university leaders to consider as they create or evolve their interdisciplinary cybersecurity programs:

- **A need to bridge technical and policy approaches:** While subject-matter focus and curriculum depth vary across programs studied, all programs offer (and nearly all require) coursework spanning both policy and technical cybersecurity topics. Focus group participants underscored the importance of educating cybersecurity students with a holistic understanding of cybersecurity: a "tech-informed" approach to cybersecurity policy, and awareness of legal and policy evolution impacting day-to-day management and development of technology. In addition, in many programs, between a quarter to one-half of courses offered are not cybersecurity-specific classes, underscoring the inherently interdisciplinary nature of cybersecurity and its relevance across the span of human experience.

- **Teaching programming through a security lens:** Computer programming requirements and approaches vary by school and degree. Bridge courses help expand accessibility into the cybersecurity domain for students with non-computer science backgrounds, and can introduce programming

[1] Hewlett Foundation,"Cyber Initiative," (Nov 2017), https://hewlett.org/wp-content/uploads/2017/11/Cyber-Initiative-Grantmaking-Strategy-11.2017.pdf.

[2] See Appendix A for focus group input.

through a cybersecurity lens to avoid security pitfalls often encountered in generic programming courses, such as when students learn to design for expected use without accounting for malicious or other unintended behavior. Some focus group participants endorsed starting with a networking approach to technical curricula, emphasizing the connections between systems and components and teaching programming as needed, rather than starting with programming as the entry to technical coursework.

- **Hands-on learning opportunities promote real-world skills:** Hands-on experiential learning opportunities, such as capstone projects, practicum courses, clinics, internships, and case studies based on actual cyber incidents, law, and global political events, help students engage in interdisciplinary problem solving. Cybersecurity clinics in particular attract and train multidisciplinary security practitioners by shifting focus from protecting assets to defending people.

- **Programs should be globally scoped and teach students to apply foundational concepts in new contexts:** To maintain relevance in the notoriously fast-evolving and globally connected field of cybersecurity, programs need to enhance US-centric cyber policy analysis with international cybersecurity perspectives, and adopt a planned strategy for curriculum revision that leads students to practice applying foundational principles and persistent cybersecurity skills (e.g., basic cryptographic math, landmark legal cases and incidents, and skills in policy analysis, development, and writing) to evolving technical and societal contexts. Proactively and transparently framing this balance to students as a benefit to their own career longevity helps to counter bias against subject material from beyond the current news cycle.

- **A need for more policy in cybersecurity curriculum frameworks:** A variety of frameworks have been developed to guide the design of academic degree programs by organizing cybersecurity into a comprehensive schema of topics and categories. These frameworks tend to address cybersecurity policy topics sparingly relative to technical cybersecurity topics. Legal aspects of cybersecurity, cybersecurity's role in foreign policy and global affairs, and cyber risk management are three broad realms under the umbrella of cybersecurity policy that are required or offered in almost all of the programs we studied, and warrant coverage in greater detail in curriculum frameworks. The majority of programs studied also offer at least one course covering privacy, cyber crime, and cyber ethics. More comprehensive definition of these sub-domains of cybersecurity policy, and acknowledgment of interdisciplinary cybersecurity degrees in accreditation and recognition programs, would help move the field of interdisciplinary cybersecurity policy from niche to mainstream.

We welcome feedback and collaboration on the topic of interdisciplinary cybersecurity education. Please email Lisa Ho, Academic Director of the Masters in Information and Cybersecurity at UC Berkeley, at lisaho@berkeley.edu.

I. Introduction

DESCRIPTION AND PURPOSE

Cybersecurity is a "wicked" problem, an intractable and complex knot of interdependencies where tugging at any one string to solve an issue creates or reveals new problems among intertwined technical, economic, legal, national security, civil liberty, and ethical issues. Simultaneously, the cumulative scope of cybersecurity threats has escalated exponentially over the past decade, yet responsibility for managing cybersecurity is left to individual users, businesses, and civic organizations.[3] In effect, each of us is protecting our corner of the digital universe by holding an umbrella against a tsunami of risks and attacks. Systemic reform, through long-term national and international cybersecurity policy that engages productively in the perpetual tussle of competing interests, is necessary for real and substantive progress.

The U.S. Office of the National Cyber Director (ONCD) has compared the need for systemic reform in the cybersecurity ecosystem to the crisis in the natural environment, asserting in a strategic intent statement: "just as individual households working to reduce their carbon footprints cannot alone address climate change, individual users of the internet working to improve their cybersecurity cannot alone realize systemic reform."[4]

In 2014, the William and Flora Hewlett Foundation recognized that the exponential escalation of cybersecurity threats was leading to an erosion of public trust in computer systems and infrastructure. Hewlett launched the Cyber Initiative with the goal of building a field of cyber policy experts with the necessary training to think about long-term national and global cyber policy and to "come up with the analytic frameworks to have an informed debate and therefore prevent short-term, reactionary policy decisions."[5]

> "We cannot continue managing these [cybersecurity] risks as we have: frantically putting fires out as they appear, never knowing for sure when or where the next one is coming — or in what form. We need established institutions with independence

[3] The White House, "A Strategic Intent Statement for the Office of the National Cyber Director," (October 28, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf.

[4] Ibid. See also: Michael Daniel, "Why Is Cybersecurity So Hard?" *Harvard Business Review* (May 22, 2017), https://hbr.org/2017/05/why-is-cybersecurity-so-hard.

[5] Eli Sugarman, quoted in "The Hewlett Foundation's Cyber Talent Pipeline," (April 2021), https://hewlett.org/wp-content/uploads/2021/07/Final-Cyber-Evaluation-2021.pdf.

> and depth of expertise to anticipate, analyze, and address the risks thoughtfully and systematically."[6]

Over the ensuing years, the Hewlett Foundation allocated grants to universities to create a talent pipeline to produce cybersecurity professionals with a mix of technical and non-technical skills, knowledge, and depth of expertise to address the competing values and trade-offs inherent in the cybersecurity problem space.

This report is intended as a guiding document for educational institutions interested in creating new cybersecurity programs, or improving existing ones to cultivate interdisciplinary and policy-fluent cybersecurity expertise for advancing systemic cybersecurity reform. The authors undertook this study seeking to both share our experience with the UC Berkeley's Master of Information and Cybersecurity program and gain insights from a landscape review of other interdisciplinary programs.

DEFINITIONS, METHODOLOGY, AND SCOPE

This report compiles publicly available information (as of Spring 2023) about the academic programming offered in a selection of 17 mature degree-granting cybersecurity programs that demonstrate commitment to interdisciplinary cybersecurity education. The study group includes 15 programs located at institutions that received Hewlett Foundation Cyber Initiative Talent Pipeline funding (though grant funds may have been targeted for research or initiatives other than the degree programs themselves).

This study iteration did not include Cyber Pipeline grantees with less formalized and/or less interdisciplinary cybersecurity program offerings. When institutions offered multiple cybersecurity degrees, the programs with significant interdisciplinary curriculum offerings were selected for the study.[7]

The following programs are included in the scope of this research. Asterisks (*) identify institutions that received Hewlett funding prior to 2023 (though not necessarily for the listed program). 2023 Hewlett grantees are indicated with a double asterisk (**).

[6] Hewlett Foundation,"Cyber Initiative," (Nov 2017), https://hewlett.org/wp-content/uploads/2017/11/Cyber-Initiative-Grantmaking-Strategy-11.2017.pdf.

[7] Related cybersecurity degree programs that were not included in the study: IU - BS in Cybersecurity and Global Policy, NYU - MS in Cybersecurity, FIU - BS in Cybersecurity, and of particular interest for interdisciplinary cybersecurity: IU - MPA/MA in Cyber Risk Management, IU - JD/MS in Risk Management, CMU - MSISPM/JD,

Brown University (Brown); Computer Science Department

- Cybersecurity, MS [fully online][8]

***Carnegie Mellon University (CMU);**

- Information Security, MSIS, College of Engineering [in person][9]
- Information Security Policy & Management, MSISPM, College of Information Systems and Public Policy [in person][10]

Columbia University (C); School of Professional Studies

- Technology Management, MS, (cybersecurity electives) [in person][11]

****Florida International University (FIU);** School of International and Public Affairs

- Global Affairs (Cybersecurity and Technology Policy concentration), MA [in person][12]

***George Mason University (GMU);** College of Engineering and Computing

- Applied Information Technology, MS (Cyber Security and IT Management concentrations) [fully online][13]

***Georgia Institute of Technology (GT);** Schools of Cybersecurity and Privacy; Computer Science; Engineering and Computer Engineering; and Public Policy

- Cybersecurity, MS [fully online or in-person][14]

***Indiana University (IU);** Luddy School of Informatics, Computing, and Engineering; Kelley School of Business; Maurer School of Law

- Cybersecurity Risk Management, MS [hybrid or fully online][15]
- *Johns Hopkins University (JHU);
- Strategy, Cybersecurity, and Intelligence, MA, School of Advanced International Studies [in person][16]
- Cybersecurity, MS, School of Engineering [fully online][17]

***New York University (NYU)**; School of Professional Studies

- Global Security, Conflict, and Cyber Crime, MS [in person or fully online][18]

[8] https://graduateprograms.brown.edu/graduate-program/cybersecurity-scm

[9] https://www.cmu.edu/ini/academics/msis/index.html

[10] https://www.heinz.cmu.edu/programs/information-security-policy-management-master/

[11] https://sps.columbia.edu/academics/masters/technology-management/master-science

[12] https://maga.fiu.edu/program/cyber-security-policy/

[13] https://catalog.gmu.edu/colleges-schools/engineering-computing/school-computing/ information-sciences-technology/applied-information-technology-ms/#text

[14] https://catalog.gatech.edu/programs/cybersecurity-ms/ Georgia Tech offers three specializations from different schools: The School of Computer Science (CS) offers the MS Cybersecurity degree with an information security specialization. The School of Electrical and Computer Engineering (ECE) offers the MS Cybersecurity degree with cyber-physical systems specialization. The School of Public Policy (PUBP) offers the MS cybersecurity degree with a policy specialization. Classes from all three were included in this study.

[15] https://cyberrisk.iu.edu/

[16] https://sais.jhu.edu/academics/master-degrees/master-arts-strategy-cybersecurity-and-intelligence- masci

[17] https://ep.jhu.edu/programs/cybersecurity/

[18] https://www.sps.nyu.edu/homepage/academics/masters-degrees/ms-in-global-security--conflict--and- cybercrime.html

***Pennsylvania State University (PSU);**

- Cybersecurity Analytics and Operations, BS, College of Information Science and Technology [in person][19]
- Engineering, Law, and Policy (ME), College of Engineering, the School of International Affairs, and Penn State Law at University Park [in person][20]

***Stanford University (S);** Institute for International Studies

- International Policy, MIP [in person][21]

***Tufts University (Tufts);** Department of Computer Science and Graduate School of Global Affairs

- Cybersecurity and Public Policy, MS [in person][22]

***University of California, Berkeley (Cal/UC Berkeley);** School of Information

- Information and Cyber Security, MICS [fully online][23]

***University of Texas, Austin (UT);** School of Law

- Cybersecurity Law Concentration, LLM [in person][24]

The Hewlett Foundation defines **"cyber policy"** broadly to include "not only traditional notions of computer and information security, but also the full range of related policy issues, such as Internet governance, net neutrality, encryption, surveillance, and privacy."[25] This study employs Hewlett's broad definition of cyber policy in recognition of the breadth of policy issues that impact cybersecurity and the need for cybersecurity policy experts to be "at the table" and well-informed during the broadest array of technology discussions.

Grantees' **"interdisciplinary"** or **"multidisciplinary"** cybersecurity programs fall along a continuum between those that offer cyber-focused classes in multiple departments or schools across the university (e.g., political science, business, law, or human behavior), those with curriculum requirements for students to take cybersecurity courses across multiple disciplines, and those that intentionally combine multiple disciplines in cybersecurity courses offered to students across schools and departments. The 2021 Hewlett Cyber Talent Pipeline Report defines the latter as a fully interdisciplinary cybersecurity curriculum.[26]

[19] https://bulletins.psu.edu/undergraduate/colleges/information-sciences-technology/cybersecurity-analytics-operations-bs/

[20] https://www.sedi.psu.edu/academics/graduate/melp.aspx

[21] https://fsi.stanford.edu/masters-degree

[22] https://engineering.tufts.edu/cs/current-students/graduate/ms-and-combined-degree-programs/ms-cybersecurity-and-public-policy

[23] https://ischoolonline.berkeley.edu/cybersecurity/

[24] https://law.utexas.edu/master-of-laws/

[25] Hewlett Foundation,"Cyber Initiative," (Nov 2017), https://hewlett.org/wp-content/uploads/2017/11/Cyber-Initiative-Grantmaking-Strategy-11.2017.pdf.

[26] "The Hewlett Foundation's Cyber Talent Pipeline," (April 2021), pgs 12–14, https://hewlett.org/wp-content/uploads/2021/07/Final-Cyber-Evaluation-2021.pdf.

The research looked across core required coursework, electives, concentrations of study, and school/department affiliation to identify trends and distinctions in the curricular offerings of the programs. When readily available, we collected syllabi (see Appendix C) and related materials; however, because we found only a small number of syllabi, we did not conduct cross-program analysis at this level of detail. We omitted general education courses required by all university students (e.g., English writing) from analysis.

The collected source material was organized in a structured repository to create a standardized view of each program. Then, a qualitative data coding process, based on a comprehensive codebook to ensure consistency and standardization, was applied to collected descriptions. This technique involved systematically identifying key themes, topics, and characteristics of each course, based on the eight knowledge areas defined in the cybersecurity curriculum development guidelines published in 2017 by the Computing Curricula Series Joint Task Force on Cybersecurity Education (CSEC2017):[27]

- Data Security
- Software Security
- Component Security
- Connection Security
- System Security
- Human Security
- Organizational Security
- Societal Security

We analyzed the categorized and labeled data to identify areas of convergence and divergence in core required coursework, electives, concentrations of study, and school/department affiliation, and to develop a better general understanding of the interdisciplinary cybersecurity curriculum landscape. We have supplemented collected data with qualitative input gathered via two focus groups and a follow-up survey with representatives from the studied programs. The findings from our analysis are presented in this report.

[27] Cybersecurity Curricula 2017 (December 31, 2017), https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf. The NICE Cybersecurity Workforce Framework work role categories (see Appendix E) were considered as alternative coding terms. Ultimately, the CSEC2017 knowledge areas were chosen for their closer alignment with university course descriptions.

LIMITATIONS

The following factors impacted our interpretations and conclusions:

- Data collected from public-facing websites may have been outdated or incomplete and may have changed during or after the investigation period (January–April 2023).
- Multiple program options at any given university complicated the straightforward representation of program requirements. We provide footnotes to explain choices taken in reporting. For example, we opted to exclude electives from programs with a very broad range of electives. In some cases, electives were offered through affiliated schools and not explicitly listed in the curriculum. We also omitted concentrations unrelated to cybersecurity. Programs without electives represented in the report include Carnegie Mellon, Indiana, Johns Hopkins MS, Penn State MEng, and Stanford.
- Interpretation of available information about courses may have resulted in mischaracterization of whether the class material was technical in nature or not, or which knowledge area or policy topics were relevant to the class. When data was missing or incomplete, analyses were made using available course titles, context, department, etc.
- Interpretation of standards and frameworks could lead to differences in conclusions.
- Available time and resources limited the number of programs that could be included in the study.
- This study does not attempt to evaluate curriculum effectiveness or program success in achieving learning outcomes. We present an analysis of program curricula data as a statement of current practice and invite report readers and program administrators to assess the suitability of program design and implementation independently.

II. Observations and Analysis

OVERVIEW

The programs selected for inclusion in this study varied significantly in composition and structure. Because of the wide diversity in program offerings, the most prominent conclusion of the study may be that few trends or meaningful averages emerge by comparing curricula across institutions, and that a wide array of models and structures are feasible. Those designing new interdisciplinary cybersecurity degrees may find the greatest value from this report as a consolidated source of information for comparing and identifying desired program characteristics, and hyperlinking to individual programs and courses for in-depth review.

Highlights of our findings and recommendations are summarized here and detailed further in the sections below:

Academic Discipline and Interdisciplinary Focus: Not surprisingly, programs based in computer science and engineering schools and colleges offer the broadest number and percentage of technical courses, and allow and require more technical courses to count toward their degrees than programs based in schools of law, international studies, and public affairs. The inverse also tends to hold, as programs based in schools of law, international studies, and public affairs skew toward policy courses more than do programs based in computer science and engineering schools. Programs based in multidisciplinary schools and programs that are jointly run by multiple schools vary in the quantity and percentage of policy and technical course offerings and degree requirements.

Cyber-Specific, Cyber-Related, and Not Cybersecurity Course Offerings: Underscoring the inherently interdisciplinary nature of cybersecurity and its relevance across the span of human experience, in most programs, between 50 and 75 percent of curricular offerings are cybersecurity-specific, with remaining coursework either touching cybersecurity as a related topic or adding contextual breadth that is not cybersecurity-specific.

Programming Requirements: Most MS degrees studied require programming coursework, while the LLM, MA, MEng, and some MS degrees do not. Bridge courses help expand accessibility into the cybersecurity domain for students with non-computer science backgrounds, and can introduce computer programming through a cybersecurity lens to avoid security pitfalls often encountered in generic programming courses (e.g., designing for expected use without accounting for malicious or other unintended behavior). Some focus group participants endorsed starting with a networking approach to technical curricula, emphasizing the connections between systems and components and teaching programming as needed, rather than starting with programming as the entry to technical coursework.

Hands-on Courses: Twelve of the 17 programs studied offer practical application and multi-dimensional problem-solving learning opportunities in the form of capstone projects, clinics, and practicums.

Curricular Frameworks: Existing cybersecurity curriculum frameworks provide less guidance regarding cybersecurity policy curricula and classes design than technical cybersecurity curricula and classes. The most policy-robust guidance is the Association for Computing Machinery Joint Task Force on Cybersecurity Education Cybersecurity Curricula 2017 (CSEC2017). Policy topics in CSEC2017 are concentrated in the "Societal Security" knowledge area, and sprinkled through three additional knowledge areas. Risk management and leadership topics are found in the "Organizational Security" knowledge area.

Policy Topics: Roughly half of all policy classes across the programs touch on the topics of cyberlaw/cybersecurity law and geopolitical cybersecurity policy. All programs require or offer at least one cybersecurity law class. The majority of programs offer at least one course that covers each of the following topics: geopolitical cybersecurity policy, organizational security, cyber crime, privacy, and cyber ethics.

ACADEMIC DISCIPLINE AND INTERDISCIPLINARY FOCUS

As shown in Table 2.1, programs included in the study demonstrate multiple approaches to an interdisciplinary cybersecurity curriculum, from programs based in the traditional technical disciplines of computer science and engineering (top yellow rows), to programs based in traditionally policy-focused disciplines of law, international studies, and public affairs (bottom blue rows), to those in multidisciplinary schools of professional studies and information (middle purple rows), and programs offered jointly by multiple schools (middle green rows).

Programs by Discipline

UNIVERSITY	DEGREE	COLLEGE OR SCHOOL	DEGREE NAME (LINK)	TECHNICAL CLASSES				POLICY CLASSES			
				# offered	% of catalog	Max allowed	Min allowed	# offered	% of catalog	Max allowed	Min allowed
Computer Science/Engineering Schools (CS/Eng)											
George Mason (GMU)*	MS	College of Engineering and Computing	Applied IT (Cyber & IT Mgmt conctr)	27	66	10	8	4	10	2	0
Brown (Brown)	MS	Computer Science Department	Cybersecurity	22	64	7	2	6	18	6	1
Carnegie Mellon (CMU)*	MSIS	College of Engineering	Information Security	15	68	4	3	5	23	3	1
Johns Hopkins (JHU)*	MS	School of Engineering	Cybersecurity	34	71	9	2	3	6	3	1
Multidisciplinary Schools (Multi)											
Columbia (C)	MS	School of Professional Studies	Technology Management (cyber elect)	3	16	3	1	3	16	3	2
New York (NYU)*	MS	School of Professional Studies	Global Security, Conflict, and Cyber Crime	2	6	2	1	21	68	8	3
UC Berkeley (Cal)*	MICS	School of Information	Information and Cyber Security	7	50	7	4	2	14	2	1
Penn State (PSU)*[28]	BS	College of Information Science and Technology	Cybersecurity Analytics and Operations	22	76	16	12	5	17	5	5
Carnegie Mellon (CMU)*	MSISPM	College of Information Systems and Public Policy	Information Security Policy & Management	15	50	15	5	3	10	3	3
Joint Schools (Joint)											
Indiana (IU)*	MS	Informatics, Computing, and Eng/ Business/ Law	Cybersecurity Risk Management	13	43	4	0	12	40	6	1
Georgia Tech (GT)*	MS	Cyber&Privacy/ CS/ Eng&CompEng/ Public Policy	Cybersecurity	18	56	7	1	8	25	5	1
Penn State (PSU)*	MEng	College of Eng/ Sch International Affairs/ Law	Engineering, Law, & Policy	7	47	4	1	6	40	6	4
Tufts (Tufts)*	MS	Dept CompSci/ Grad School of Global Affairs	Cybersecurity and Public Policy	29	48	7	3	31	51	7	3
Law/International (Law/Intl)											
UT Austin (UT)*	LLM	School of Law	Laws (Cybersec Law conctr)	2	13	2	1	13	81	4	1
Stanford (S)*	MA	Institute for International Studies	Internat'l Policy (CyberPolicy&Sec specializ)	6	19	3	0	13	39	10	7
Florida Internat'l (FIU)**	MA	School of International and Public Affairs	Global Affairs (Cyber & Tech Policy conctr)	1	7	1	1	5	33	5	5
Johns Hopkins (JHU)*	MA	School of Advanced International Studies	Strategy, Cybersecurity, and Intelligence	1	4	1	0	19	79	6	4

Table 2.1 Programs grouped by discipline of the school(s) or college(s) offering the degree, with a breakdown of technical and policy classes offered (count and percentage of course catalog) and minimum and maximum number of policy and technical classes that can be counted toward the degree. Asterisks identify institutions that have received Hewlett Foundation funding (though not necessarily for the listed program).

[28] As a four-year Bachelors program, the Penn State BS has an overall greater number of course requirements than the other programs studied (which are otherwise masters degrees).

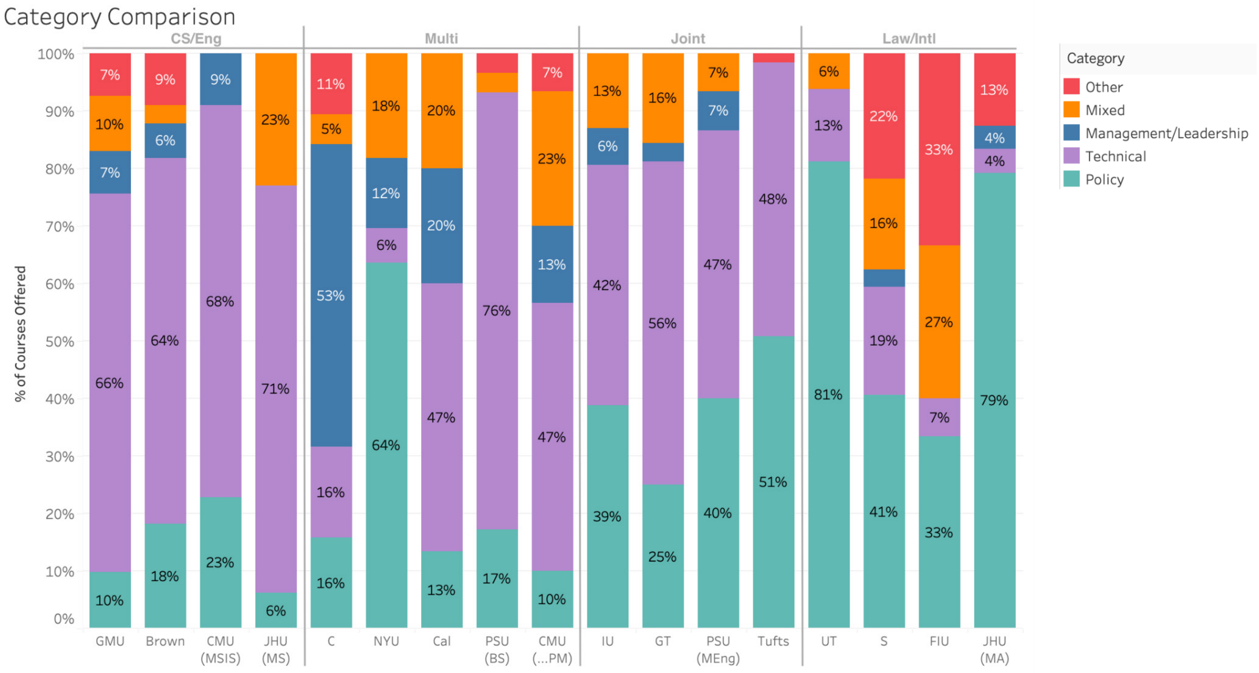
Looking at the relationship between course offerings and the discipline of the school(s) or college(s) offering the degree, a variety of trends emerge:

- Not surprisingly, programs based in schools and colleges of computer science and engineering (CS/Eng) offer a greater number and percentage of technical courses compared to programs offered by schools of law, international studies, and public affairs (Law/Intl). Programs offered by multidisciplinary schools (Multi) or jointly by multiple schools (Joint) fall along a spectrum between a technical and policy focus. (See Figures 2.1 and 2.2.)
- Programs based in CS/Eng schools also allow students to count more technical classes toward their cybersecurity degrees, and require that students take more technical coursework. Only three programs do not require technical classes (see Figure 2.2).
- Similarly, Law/Int host schools generally predict a focus on policy in their curricular offerings and percentage of the course catalog, while CS/Eng schools generally offer fewer policy classes. Multidisciplinary and joint school programs generally fall in the middle, with notable exceptions (Tufts, NYU).
- All but one of the 17 programs (George Mason) require policy coursework. Law/Intl as well as Multi and Joint programs tend to allow and require more policy courses to count toward their degrees than do CS/Eng programs.

Across the variety of program structures and curriculum foci, the majority of programs require coursework spanning both policy and technical topics. Although there is a range of programming requirements across programs, focus group participants endorsed a “tech-informed” approach to cybersecurity policy curricula and a systems focus for technical coursework.

Figure 2.1 depicts the percentage of courses offered in each category of policy, technical, leadership/management, mixed (combination of technical and management topics), and other. Classes that combine policy with other categories are included in the policy category. For example, 81% of courses in the course catalog at UT Austin (Law) are policy classes, while just six percent of courses in Johns Hopkins’ MS program are policy-focused.

Course Catalog by Category



Total catalog count:	41	33	22*	48*	19	33	15	29	30*	31*	32	15*	61	16	32*	15	24

** Total catalog count excludes electives for specified programs*

Figure 2.1 Course category breakdown, based on the total number of classes offered in each program.

Policy and Technical Course Counts and Requirements

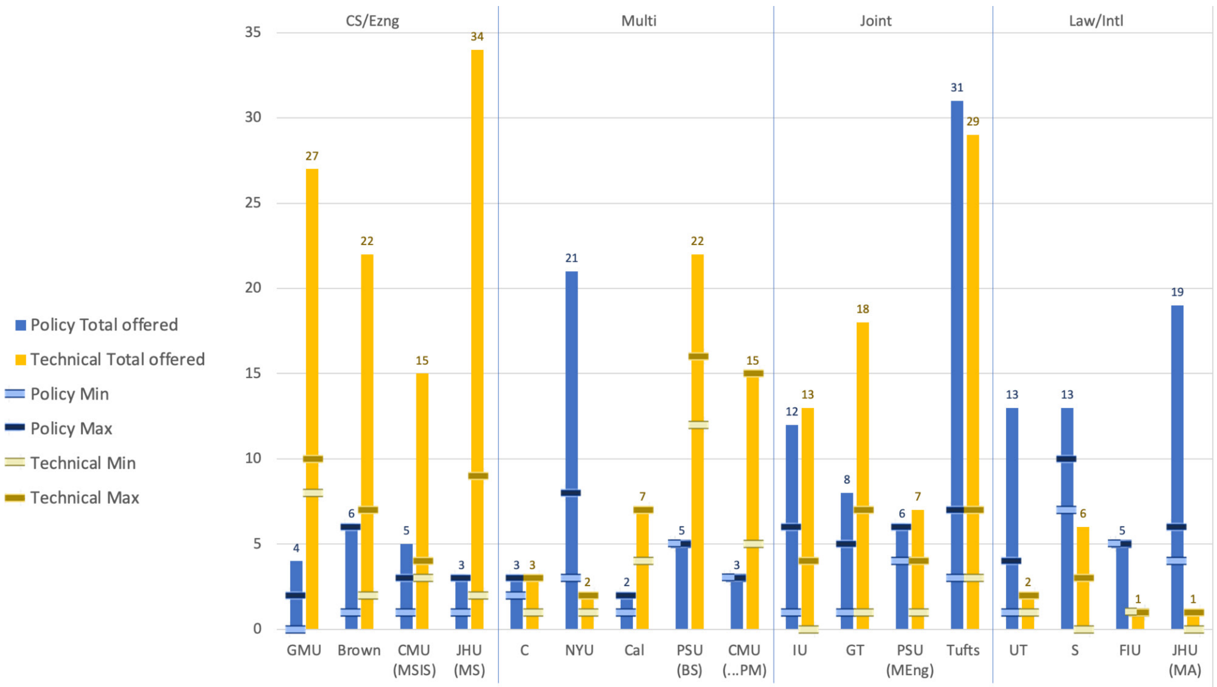


Figure 2.2 Policy vs technical course counts and minimum required and maximum allowed courses that count toward the degree.

Figure 2.2 depicts the total count of technical and policy courses offered at each institution, and the maximum and minimum number of courses in each category that a student could take according to their program's requirements. Classes in management, mixed (technical and management), and other categories are not included.

For example, one program (George Mason) does not require students to take any policy courses to accomplish their degrees (as shown by the light blue horizontal "Policy Min" bar at 0), and allows students to take a maximum of 2 (dark blue horizontal "Policy Max" bar) of the 4 total policy classes offered toward their degree (indicated by the 4 label above the vertical blue column).

CYBERSECURITY-SPECIFIC, CYBER-RELATED, AND NOT-CYBERSECURITY COURSE OFFERINGS

When reviewing programs' course catalogs, we found it valuable to consider whether or not coursework focused specifically on cybersecurity.

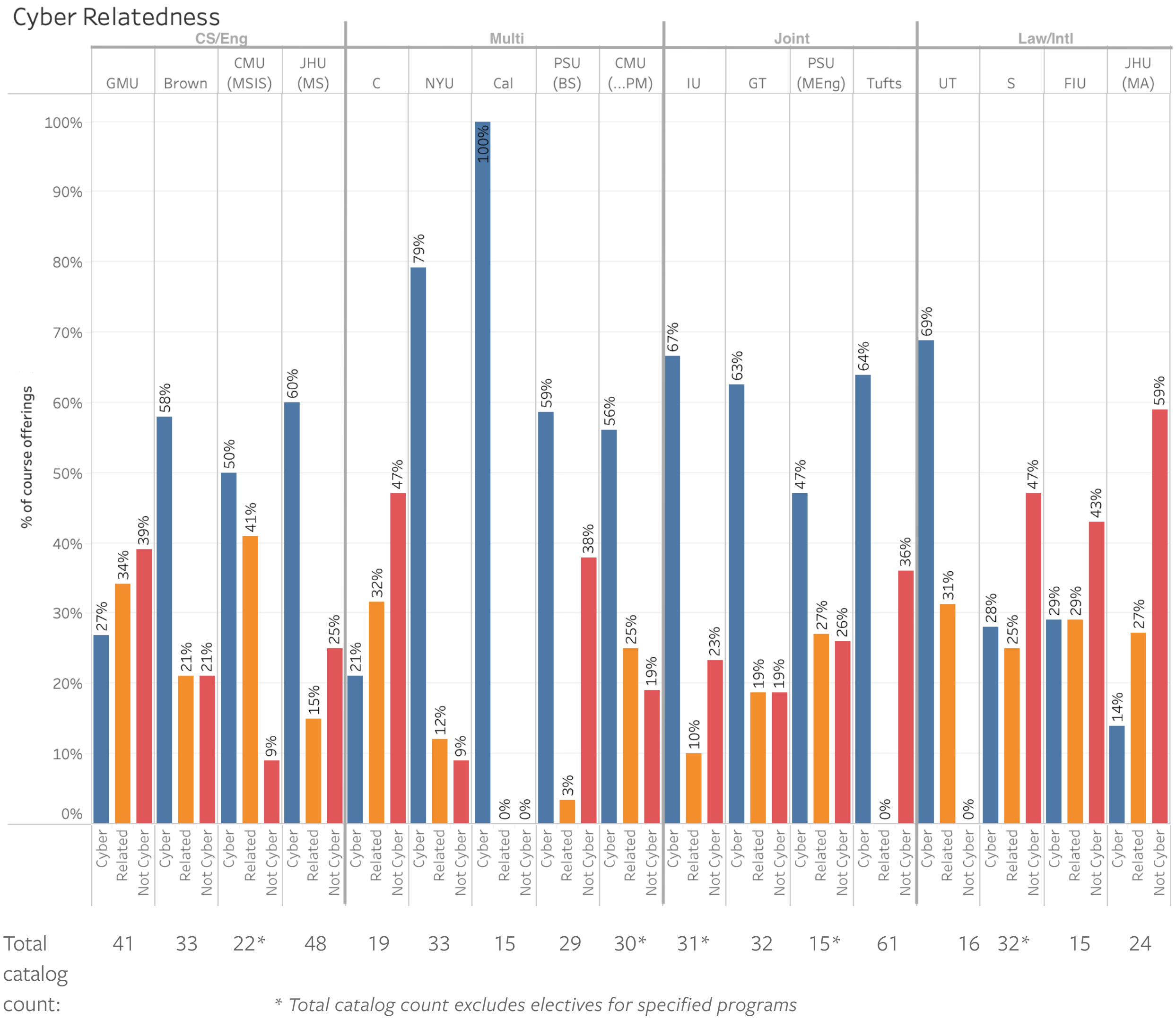
Some programs with a more prescribed curriculum (i.e., smaller course catalog) had a higher percentage of cyber-specific courses than other programs that had a broader course catalog and relatively lower percentage of cyber-specific courses. For example, at UC Berkeley, the total catalog count was 15 courses, with 100% cyber-specific classes, while at George Mason, 27% of the 41 courses offered were cybersecurity-specific. However, other programs counter this association (e.g., Tufts: 61/64%, Florida International: 14/29%). Therefore, a university's breadth of course offerings or depth in policy or technical coursework does not predict the percentage of cyber-specific courses offered.

For the bulk of programs (excluding outliers Columbia, George Mason, Johns Hopkins MA, Florida International, Stanford, and UC Berkeley), one-half to three-quarters of course offerings are cybersecurity-specific. Remaining coursework either touches cybersecurity as a related topic or adds contextual breadth that is not cybersecurity-specific, underscoring the inherently interdisciplinary nature of cybersecurity and its relevance across the span of human experience.

In Figure 2.3:

- Cybersecurity-specific offerings (**Cyber**) indicate courses with the majority of course content directly focused on cybersecurity (e.g., a course titled "Network Security").
- Cybersecurity-related offerings (**Related**) indicate courses that are related to cybersecurity but have primary foci elsewhere (e.g., a course titled "International Policy and Law" that mainly focuses on global affairs and touches on cybersecurity topics such as privacy or surveillance).
- Non-cybersecurity course offerings (**Not Cyber**) indicate courses that are not directly related to cybersecurity and do not explicitly touch on cyber topics, but are still included in a program's curricula (e.g., a course titled "Work and Employment Relations in the 21st Century").

Course Catalog Cyber-relatedness



* *Total catalog count excludes electives for specified programs*

Figure 2.3 Percentage of courses categorized as cyber-specific, cyber-related, or not cyber for each program, with the total number of courses in the program displayed.

PROGRAMMING REQUIREMENTS

Programs vary regarding expectations for students' and applicants' computer programming skills, reflecting the range of program foci, target career outcomes, and institutional philosophies. Several focus group participants asserted that generic programming courses are not ideal technical introductions for cybersecurity policy students because they potentially ignore security pitfalls (for example, students may learn to design software without accounting for malicious or other unintended behavior), and do not sufficiently address the networking and systems knowledge fundamentals of cybersecurity (see Appendix A: Focus Group Feedback). Eleven programs do not list programming skills in admissions requirements and do not require coursework with programming prerequisites:

Brown (Policy Track)
Columbia
Carnegie Mellon MSISPM
Florida International
George Mason[29]
Indiana
Johns Hopkins MA
NYU
Penn State MEng
Stanford
UT Austin

The following seven programs state programming requirements for entrance or require coursework that specifies programming prerequisites. The programs at Tufts, Johns Hopkins, and George Mason MS[30] offer a wide range of technical courses and place emphasis on advanced programming skills in coursework.

- **UC Berkeley** — Core courses that require computer programming: Cryptography, Software Security, and Network Security.
- **Brown (computer science track)** — Requires "undergraduate-level coursework in (1) mathematics that covers calculus, discrete mathematics, and probability or statistics, and (2) introductory computer science that covers computer programming and data structures and algorithms."
- **Carnegie Mellon MSIS** — "Successful applicants . . . also typically have: A technical background or academic exposure that supports advanced study in their area of interest. Strong quantitative, analytical, and programming skills."
- **Georgia Tech** — Required course: Introduction to Information Security. Prerequisites include "experience in programming a high-level programming language.")

[29] The Georgia Mason Cybersecurity concentration requires classes with programming prerequisites, whereas the IT Management Concentration (which offers cybersecurity electives) does not require programming.
[30] See prior footnote.

- **Johns Hopkins MS** — Students are expected to have some prior programming background, but provisional admission is offered.
- Core courses that require programming: Foundations of Algorithms, Foundations of Information Assurance, and Cryptology.
- **Penn State BS** — The following required courses have programming prerequisites: Cyber-Defense Studio, Cyber Incident Handling and Response, Malware Analytics, Network Security, and Computer and Cyber Forensics.
- **Tufts** — "Students must have taken an introductory course in computer programming before enrolling in the program. This is not an admissions requirement to be accepted into the program but is an entrance requirement – if a student is accepted into the program before they have taken an introductory course in computer programming, they must take the course before they start the program."

Programming Bridge Courses

UC Berkeley, Johns Hopkins' MS, and Carnegie Mellon's MSISPM require computer programming, but also admit applicants without programming experience and offer programming fundamentals classes as part of the degree program.

- **UC Berkeley** — "Knowledge of at least one, and ideally two, programming languages, such as C, C++, Python, Java, Javascript, or machine/assembly language as demonstrated by work experience or coursework. Applicants who lack this experience in their academic or work background are encouraged to take the Programming Fundamentals for Cybersecurity course in their first term. Students may opt-in or out of this course."
- **Johns Hopkins MS** — "Applicants whose prior education does not include the prerequisites listed under Admission Requirements may still be admitted under provisional status, followed by full admission once they have completed the missing prerequisites." Introduction to Programming using Java and Introduction to Programming Using Python are offered, but are not counted toward degree completion.
- **Carnegie Mellon MSISPM** — Introduction to Programming with Python ("designed for students with little or no programming knowledge") and Software and Security (exposes students with limited exposure to programming to basic programming constructs) are both core classes in the MSISPM curriculum.

CAPSTONE, PRACTICUM, AND CLINICAL COURSE OFFERINGS

Most programs offer or require hands-on, experiential learning opportunities such as capstone projects, clinics, practicums, and internships that give students the real-world, project-based experience in cybersecurity sought by employers. Such courses exercise practical application and multi-dimensional problem-solving skills that are critical for cybersecurity policy. The programs below have established courses in the following hands-on learning models (note that the categories are not mutually exclusive). Hyperlinks to further course information are included in the electronic version of this report.

Clinics

Cybersecurity clinics are an adaptation of law and medical school clinics, where students work with real-world clients with limited resources and gain valuable hands-on experience. Cybersecurity clinics train students from diverse backgrounds and academic expertise to strengthen the digital defenses of non-profits, hospitals, municipalities, small businesses, and other under-resourced organizations in our communities, while also developing a talent pipeline for cyber civil defense. The Consortium of Cybersecurity Clinics (cybersecurityclinics.org) provides resources and support for institutions interested in the cybersecurity clinic model.

- UC Berkeley: Public Interest Cybersecurity: The Citizen Clinic Practicum
- Indiana: Cybersecurity Clinic
- UT Austin: Applied Cybersecurity Community Clinic

Practicums

Practicums offer hands-on experiential learning experiences working with partners or clients in commercial, industrial, academic, government, and other settings on real-world issues.

- UC Berkeley: Web Application Security Assessment Practicum (testing campus systems)
- Georgia Tech: Info Security Practicum
- Indiana: Information Privacy & Security Management Practicum
- NYU: MSGSCC Consulting Practicums
- Penn State MEng: Engineering, Law, and Technology Practicum

Capstones

Capstones are culminating courses generally requiring students to synthesize their program studies for application to real-world challenges and opportunities. Work may take the form of team-based projects, case studies, client work, written research, or other major endeavors.

- UC Berkeley: MICS Capstone
- Columbia: Technology Management Capstone Project
- Carnegie Mellon MSISPM: Information Security Capstone Project
- Florida International: Capstone
- George Mason: Capstone Seminar (case analysis)
- Indiana: Capstone & Practicum (case studies, simulations and client engagements)
- Johns Hopkins MA: Capstone (research thesis or brief)
- NYU: Capstones and Internships
- Penn State BS: Capstone
- Stanford: MIP Capstone Policy Change Studio (MIP Problem-Solving Framework)

Other

- Stanford: Cyber Policy Fundamentals (simulations and scenario exercises)
- Stanford: Required hands-on Hack Lab
- Carnegie Mellon: Advanced industry-sponsored projects
- Internships

CYBERSECURITY CURRICULUM FRAMING

To further analyze course offerings, we categorized classes in each program's course catalog based on the eight knowledge areas defined in the Association for Computing Machinery Joint Task Force on Cybersecurity Education Cybersecurity Curricula 2017 (CSEC2017).[31] These knowledge areas are detailed in Appendix F. This framework provides more specificity regarding cybersecurity policy topic areas than other standards we considered. (See our recommendation below: "Enhance and Infuse Policy into Cybersecurity Frameworks.")

[31] https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

Distribution of Curriculum Topics

For all classes listed in each program's cybersecurity degree course catalog, we assigned a single top-level cybersecurity "Primary Topic" from the eight CSEC2017 knowledge areas and multiple "Secondary Topic" knowledge areas (using course descriptions and other available materials as source data). See Appendix D for each program's course catalog breakdown by knowledge area.

Primary topics across courses and programs

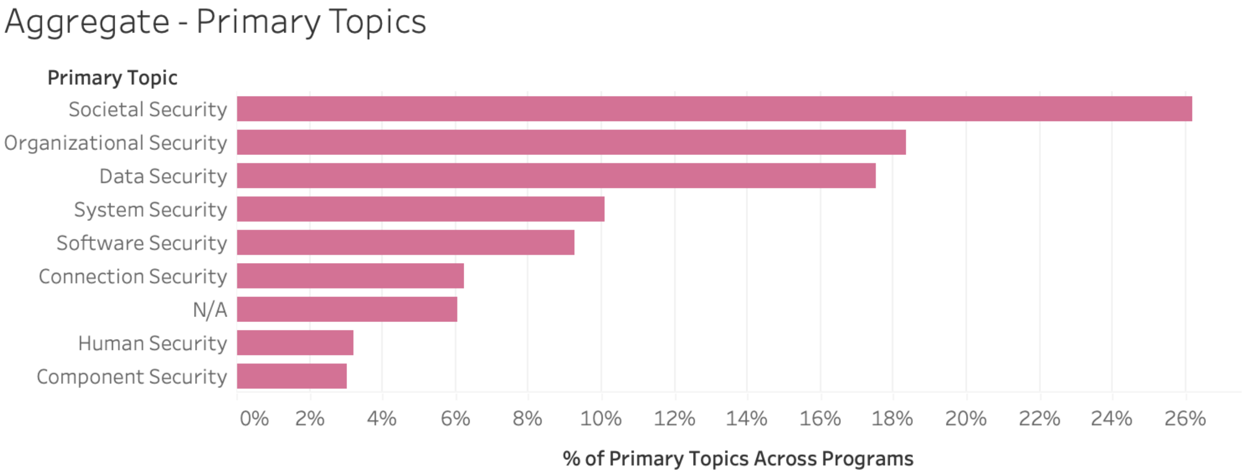


Figure 2.4 Primary topics across all classes in all programs.

Across all course offerings from all programs studied, courses with Societal Security as the primary topic were most prevalent, followed by Data Security and Organizational Security, adding up to over 60% of the total course offerings across these three Knowledge Areas.

Two factors contribute to the prominence of Societal Security as a primary topic: 1) this study's focus on interdisciplinary cybersecurity policy programs, and 2) the concentration of nearly all law and policy topics in the Societal Security Knowledge Area within the CSEC2017 framework, compared with multiple technical Knowledge Areas that are more granularly defined.

The next most common primary topic, Organizational Security, reflects programs' professional orientation, prioritizing the application of cybersecurity within an organizational context. For example, Risk Management is a topic relevant for both technical and policy-oriented cybersecurity practitioners.

The N/A value represents courses such as capstones, seminars, and practicums that do not have a predefined primary topic.

Secondary topics across courses and programs

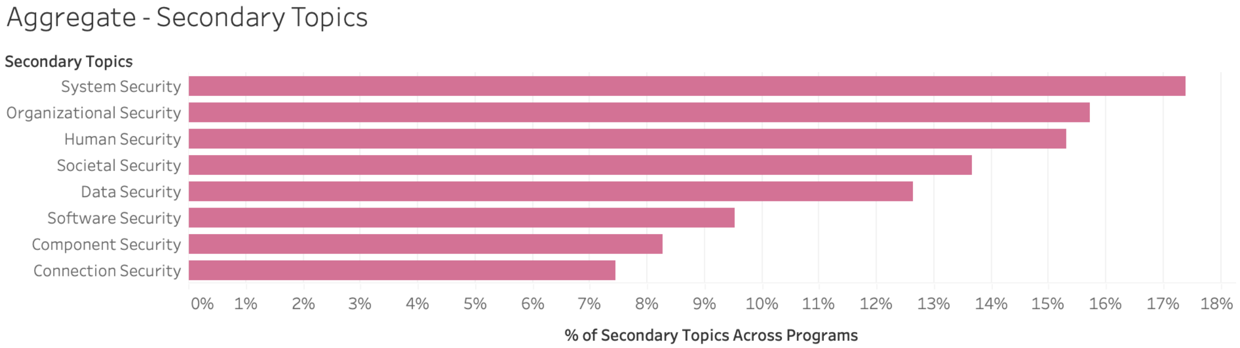


Figure 2.5 Secondary topics across all classes in all programs.

Each course was also assigned any number of secondary topics, as applicable, from the remaining CSEC2017 knowledge areas. Some courses had no secondary topics.

System Security is the most common secondary topic; this reflects curricular decisions to imbue technical cybersecurity courses with an emphasis on holistic thinking regarding the interactions between pieces of a system, which is one of the key learning outcomes of System Security. For example, a Networking Security course would be tagged with the primary topic of Connection Security and may also require students to adopt a system-level perspective, e.g., how networking protocols may interact with a corporate IT infrastructure's security posture and risk analysis.

Similarly, Organizational Security classes also frequently include System Security topics secondarily. For example, topics in a course titled "Corporate Risk Management" would fall primarily within CSEC2017's Organizational Security knowledge area, but would likely also involve holistic thinking and system-level management, which are key sub-topics of System Security.

POLICY TOPICS

To further examine policy courses offered by the programs studied, we tagged policy classes with the CSEC2017 framework's **Organizational Security** knowledge area and the Societal Security knowledge area subtopics of **Cyberlaw** (including intellectual property law and contracts), **Cyber Policy** (cybersecurity's role in global security), **Cybercrime**, **Cyber Ethics**, and **Privacy**, which are defined in CSEC2017 as including the following subtopics:

Societal Security:

Cyberlaw: Constitutional foundation of cyber law, IP, Privacy laws, Data security law, Computer hacking laws, Digital evidence, Digital contracts, Multinational conventions (accords), Cross-border privacy and data security laws.[32]
Cyber Policy: International cyber policy, U.S. federal cyber policy, Global impact, Cybersecurity policy and national security, New adjacencies to diplomacy.
Cybercrime: Cybercriminal behavior, Cyber terrorism, Cybercriminal investigations, Economics of cybercrime.
Privacy: Defining privacy, Privacy rights, Safeguarding privacy, Privacy norms and attitudes, Privacy breaches, Privacy in societies.
Cyber Ethics: Defining ethics, Professional ethics / codes of conduct, Ethics and equity/diversity, Ethics and law, Autonomy/robot ethics, Ethics and conflict, Ethical hacking, Ethical frameworks, and normative theories.

Organizational Security:

Risk Management, Governance & Policy, Laws, ethics, and compliance, Strategy and Planning

Roughly half of all policy classes across all programs touch the topics of Cyberlaw/Cybersecurity Law and Cyber Policy.

- All programs require or offer at least one cyberlaw class. NYU(18) and Indiana (8) stand out with robust offerings in cyberlaw.
- Three quarters of programs offer at least one cyber policy class. Tufts (21) and NYU (17) stand out, along with Johns Hopkins MA, which requires four cyber policy classes.

Roughly a quarter of all policy classes across all programs address organizational security, cyber crime, and privacy as topics.

- NYU offers 10 cybercrime classes.
- Indiana offers eight classes that touch upon privacy, and Tufts requires four classes that include privacy-related topics.

[32] Focus group participants noted that in law school curricula, "cyberlaw" frequently means "internet law" (with a primary focus on intellectual property issues), while information security law is often called "cybersecurity law." In this study, we use the CSEC2017 definition of cyberlaw, which includes both internet/intellectual property and information security legal issues.

One sixth of policy classes across all programs cover cyber ethics, with more than half of all programs offering at least one course covering these topics.

- Tufts offers six classes that reference cyber ethics in their course descriptions.

Cyber policy sub-topic distribution

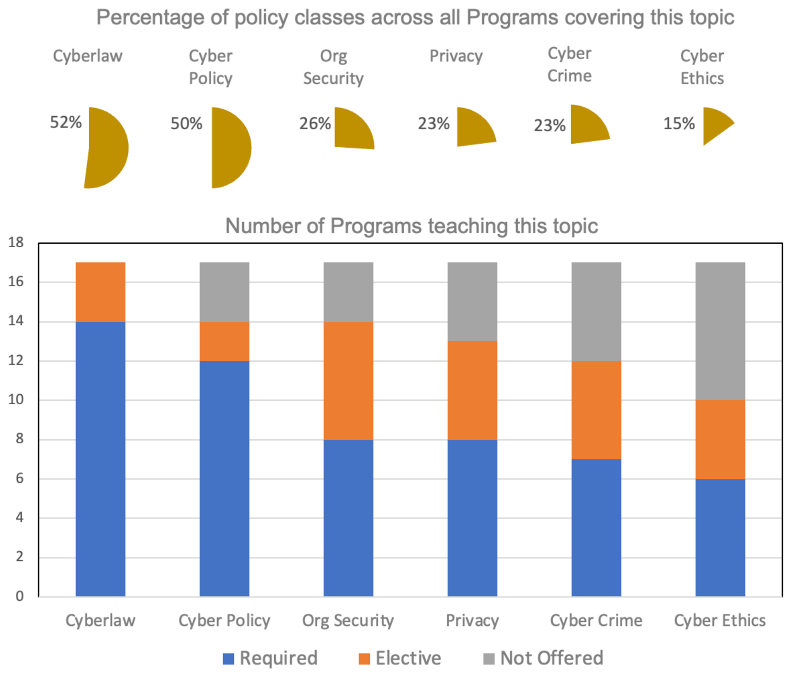


Figure 2.6 Top section: Pie charts depicting the proportion of all policy classes across all programs covering policy sub-topics, Bottom section: Bar charts depicting the number of programs teaching the policy subtopic as a required or elective course, or not offered.

NYU's Global Security, Conflict, and Cyber Crime MS degree stands out for its wide range of cybersecurity policy courses, with 18 cyberlaw, 17 cyber policy, and 10 cybercrime-related classes. Unlike other programs that have a dual emphasis on policy and traditional information security disciplines, NYU stands out with its international focus and attention to fledgling cybersecurity studies, with courses such as "Disinformation and Narrative Warfare." NYU's policy depth comes with a tradeoff: fewer technical courses are available to students compared with other programs, many of which require students to develop technical expertise to inform their future policy-making.

Tufts offers diverse options, including 21 cyber policy, six cyber ethics, and four required policy classes covering privacy. Tufts also offers a variety of policy classes that are not specific to cybersecurity within their cybersecurity degrees.

Indiana specializes in cyber law, privacy, and cybercrime, providing eight classes in each area, and the Johns Hopkins MA program requires four cyber policy classes, showcasing its focus on policy-related aspects of cybersecurity.

Carnegie Mellon has developed a fairly unique structure for its MSIS degree: rather than having a prescribed set of mandatory courses with a complementary pool of electives (as is the case at Tufts or UC Berkeley), the MSIS program has a series of "cores" (system, security, networking, and business & management), with multiple course options in each. Along with a required security course and two professional development courses, students customize their interdisciplinary experience by selecting one or more classes from each core group. While the MSIS program does not have a policy "core," CMU's Master of Science in Information Security Policy & Management (MSISPM) is available for students seeking a more robust cybersecurity policy curriculum.

While many programs offer at least one course on managing traditional business organizational cybersecurity infrastructure (e.g., risk management), UC Berkeley and Indiana offer courses on small non-profit and local government cybersecurity organizational management through their public interest cybersecurity clinics.

Appendix B lists all the policy courses offered in the programs studied. We included classes referencing any facets of cyber policy, even when secondary to the course's primary focus.

III. Recommendations

CURRICULUM RECOMMENDATIONS

While this research did not collect data to evaluate curriculum effectiveness, and the diversity of programs studied defied attempts to cull aggregate trends or best practices, we offer the following recommendations based upon our observation of the curricular offerings of the programs studied, together with general pedagogy and cybersecurity principles, and our experience developing the UC Berkeley's Master of Information and Cybersecurity degree.

Build Pathways for Diversity of Background and Thought

In distinguishing between *complicated* and *complex* operating environments, the Cynefin Framework for Decision Making[33] makes a compelling case for fostering diversity of thought, which is also applicable in the cybersecurity field. Unlike *complicated* environments, where at least one right answer exists and diagnosing cause and effect relationships is possible given sufficient expertise, *complex* environments are characterized by flux and unpredictability, and comprehension emerges only in retrospect. In complex environments like the cybersecurity domain, encouraging dissent, diversity, and interaction across divergent ideas, rather than attempting to compel predictable results, creates the capacity to identify emergent patterns when no "right" answers exist.

1. Attracting students with a diversity of experiences, academic disciplines, and demographic backgrounds, and supporting their success, requires intentionally putting in place programmatic scaffolding to support students as they enter the field. UC Berkeley, for example, successfully draws students into cybersecurity from non-technical degree programs through the Citizen Clinic, through which students help protect under-resourced non-profit organizations that serve vulnerable communities. Additionally, "bridge" courses that introduce programming, math, and other technical subjects reduce the barrier to entry for students without computer science backgrounds. Tutoring resources and co-curricular community events can also help build social and academic support networks and strengthen student engagement and resilience.
2. Offering courses from multiple departments and schools exposes students to different

[33] David J. Snowden and Mary E. Boone, "A Leader's Framework for Decision Making," *Harvard Business Review* (November 2017), https://hbr.org/2007/11/a-leaders-framework-for-decision-making.

disciplinary thinking models. Integrating multiple disciplines within individual courses offers students practice in the kind of cross-disciplinary thinking[34] needed to address complex real-world cybersecurity policy problems.

3. Culminating capstone and practicum courses, experiential learning opportunities such as cybersecurity clinics[35] and internships, and case study coursework based on real-world examples of cyber incidents, law, and global political events can all help defy mono-disciplinary thinking and help students synthesize learning from across their program into multi-disciplinary solutions.
4. Cybersecurity policy cannot be divorced from technical implementation, and technical coursework equips cybersecurity policy experts to understand realistic policy possibilities and limitations. Similarly, technical decisions have human consequences, and so exposure to policy topics is also imperative for cybersecurity technicians.

Balance Foundational and Current Topics

5. Cybersecurity is recognized as a notoriously fast-evolving field, and students rightly expect course material to be up-to-date. This necessitates a planned strategy for maintaining a curriculum that teaches students to apply foundational concepts in new contexts. To maintain relevance, programs need to adopt a planned strategy for curriculum revision that leads students to practice applying fundamental principles and persistent cybersecurity skills (e.g., basic cryptographic math, landmark legal cases and incidents, skills in policy analysis, development, and writing) to evolving technical and societal contexts. Proactively and transparently framing this balance to students as a benefit to their own career longevity helps to counter bias against subject material that falls outside of the current news cycle.

Incorporate Global Scope

6. To adequately prepare a cybersecurity workforce that is globally connected, programs should complement U.S.-centric cyber policy analysis with international cybersecurity perspectives, such as legal and regulatory factors, cultural and social factors (e.g., different perspectives on civil liberties, public safety, and surveillance), as well as economic factors and geopolitical strategies.

[34] Gregory Falco, *et al*, "Cyber risk research impeded by disciplinary barriers," *Science* (November 29, 2019), https://www.science.org/doi/abs/10.1126/science.aaz4795.

[35] Find resources and toolkits for starting a cybersecurity clinic at the Consortium of Cybersecurity Clinics, https://cybersecurityclinics.org/.

ADVOCACY RECOMMENDATIONS

While interdisciplinary policy-focused cybersecurity is still a new and niche field, the domain's importance warrants reinforcement in existing cybersecurity education frameworks that have been created to guide design of academic degree programs by organizing cybersecurity into a comprehensive schema of topics and categories. Such frameworks include:

- Association for Computing Machinery (ACM) Joint Task Force on Cybersecurity Education Cybersecurity Curricula 2017 (CSEC2017).[36]
- National Center for Academic Excellence in Cybersecurity (NCAEC) criteria.[37]
- National Initiative for Cybersecurity Education (NICE).[38]

Enhance and Infuse Policy into Cybersecurity Frameworks

The cybersecurity profession has arguably existed since system and network administrators first found themselves combating rampant internet viruses in the late 1980s, a period marked by the founding of the International Information System Security Certification Consortium, Inc (ISC)² in 1989. As a result, cybersecurity frameworks have evolved to be more robust in technical domains than policy domains.

Across the eight top-level knowledge areas in CSEC2017, cybersecurity policy topics are concentrated in the Societal Security knowledge area, with some representation and overlap in the Human Security and Organizational Security knowledge areas. Technical topics are explicated across the five remaining knowledge areas (Data Security, Software Security, Component Security, Connection Security, and System Security), with minor, if any, reference to policy topics. (For more detail on CSEC2017, see Appendix F.)

Within the NICE framework, which comprises 33 defined specialty areas, policy work is concentrated in two areas: Strategic Planning and Policy[39] and Legal Advice and Advocacy[40] (see Appendix E). On June 21, 2023, NICE proposed 15 Framework Competency Areas,[41] one of which is Cybersecurity Fundamentals, which includes the broad topics of risk management; privacy principles; policy, law, and ethics; networking and systems; digital resilience; digital literacy; and computational literacy.

[36] https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf
[37] https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_designation_requirements.pdf
[38] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce- framework-cybersecurity-nice
[39] https://niccs.cisa.gov/workforce-development/nice-framework/work-roles/cyber-policy-and-strategy- planner
[40] https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/legal-advice-and- advocacy
[41] https://www.nist.gov/system/files/documents/2023/06/14/NICEFramework_CompetencyAreas_List.pdf

We believe that more robust definition and representation of policy in CSEC2017 knowledge areas and NICE Speciality and Competency Areas would enhance the infusion of policy coursework into cybersecurity curricula. This could include establishing cybersecurity law, cybersecurity geopolitics, and cyber risk management as top-level cybersecurity knowledge or competency areas, each with multiple sub-topics defined in greater detail.

Seek Recognition of Interdisciplinary Programs

The criteria currently used in the Center for Academic Excellence - Cyber Defense (CAE-CD) designation, a certification offered by the National Security Agency, requires universities to identify their program of study as *either* technical *or* non-technical.

The five technical core knowledge units defined in the CAE-CD curriculum are:

- Basic Scripting and Programming (BSP)
- Basic Networking (BNW)
- Network Defense (NDF)
- Basic Cryptography (BCY)
- Operating Systems Concepts (OSC)

The five non-technical core knowledge units are:

- Cyber Threats (CTH)
- Policy, Legal, Ethics and Compliance (PLE)
- Security Program Management (SPM)
- Security Risk Analysis (SRA)
- Cybersecurity Planning and Management (CPM)

Revising the CAE-CD criteria to recognize and endorse degrees that require and emphasize both technical and non-technical studies would signal the critical value of interdisciplinary cybersecurity education, and likely increase the proliferation of university-based interdisciplinary cybersecurity degrees.

IV. Conclusion

To substantively address global cybersecurity threats, which increasingly transgress digital boundaries and erode social trust and safety throughout virtual cyberspace and physical "atomspace," cybersecurity policy education must mature from a niche specialty into a mainstream academic and professional discipline.

In this study, we offer a cross-sectional view of a handful of interdisciplinary cybersecurity degree programs in the U.S. In presenting this slice of the landscape, we hope to stimulate development and growth of programs designed to advance holistic cybersecurity expertise to bridge the variety of technical and human domains needed to actualize comprehensive cybersecurity solutions.

V. Appendix

A. FOCUS GROUP FEEDBACK

We convened two focus groups after compiling our research findings. These sessions involved faculty and administrators who are engaged in curriculum development from the programs studied, plus representatives from new Hewlett grantee institutions. These sessions served multiple purposes: first, to share, discuss, and validate the findings presented in our report drafts; second, to gather qualitative insights regarding interdisciplinary cybersecurity education and curriculum development; and third, to evaluate the value and appetite for ongoing engagement as a community of practice around interdisciplinary cybersecurity education with a policy focus. We also collected feedback from focus group participants via a follow-up survey. Some of the key insights from participants are included below (edited for clarity and length).

Curriculum Technical Balance

On the topics of balancing technical vs non-technical coursework, programming requirements, and whether to offer separate technical and non-technical tracks:

- We are fundamentally a policy program, and I am debating whether to keep a hands-on hacking lab mandatory. It is keyed for newbies, and much of the class is concerned with how to understand and exploit networks and the devices on them.
- We count certain CS classes as electives and encourage students to grow their technical skills through formal coursework as well as options like Coursera.
- Currently, we require very little programming, but in the future we would like to have it integrated.
- We offer two different network security courses: one for technical folks in our MS degree and one for folks in the policy & management degree
- The main plank was to launch an interdisciplinary cyber security educational program, building coursework from the ground up, designed to ensure that the law students would know some of the technology and that the engineering students would know some of the policy. We operate a program that we don’t think of as school specific: you’ve got to take some technology familiarization courses that are just tech, and some law, and some policy, and then some specialization courses.

- We thought that the most critical thing was some amount of linguistic familiarity with key technical concepts for the law, business, and policy students. And conversely, the same thing applied backwards to our engineering, information school, and computer science students. So we were very conscious and deliberate in crafting a two-track model, and that you needed to have education in both tracks.
- We wound up with different technical and non-technical tracks.
- I'm interested in the relationship between the technical/non-technical, programming versus non-programming, because our students are not going to succeed if it's an incredibly technical/programming-oriented curriculum. We're trying to figure out what two courses could be added that would introduce the cybersecurity issues that our students might deal with in the workforce, particularly in public administration and global security, because a lot of our students are going into state and federal jobs.
- I learned that I was not the only one having trouble with social science and legal postdocs coming to do tech-informed cyber security policy and then really not wanting to learn the tech. They wanted just to continue doing the cyber security policy without the tech. So I ran a workshop on Tech for Social Science and Legal Scholars.[42] It was three-and-a-half days combining tech with labs with tech talks about cybersecurity. I was the only one who talked about policy because I talked a little bit about cryptography policy. We ran the workshop without assuming that the students knew programming. We had people teaching how a system works and then giving a hands-on lab to do.
- The question I get asked from prospective students more than any other is: How much technical expertise do I need? My answer is always, "It depends on your career goals." If you're interested in deterring and combating Russian aggression in cyberspace, there is a technical element, but largely it's about understanding what makes the Russians tick, what their incentives are, what their pain points are, what tools we have to bring to bear, and how to make credible threats about using those tools. That's a very different challenge from: How does one build a software bill of materials? That's a little more technical. So I tell students, let's figure out where you are today and figure out where you want to be, and then we'll chart a path for you to get from point A to Point B. For some students that may mean they should take some programming classes, if only to familiarize themselves with the culture, which is an important thing. For other students you say, we're a policy program: you need to triple down on your policy content: do more economics to understand when I talk about asymmetric information, why that matters and why the software bill of materials and cyber security software labeling are designed to tackle that problem. Since our program is embedded in an international policy program, our core is international policy

[42] https://cspp.tufts.edu/node/971

with cyber specialization, so curriculum is more policy-oriented: economic development, democracy, rule, law, international security, trade, human rights, energy, and environment topics that are germane to international affairs.

- I'm not sure if there's gonna be a significant benefit for a cyber policy student to take an intro programming class. What *would* be beneficial is being able to take a network security class where the actual code writing is something that they pick up along the way. (I taught the Network and Security class in our interdisciplinary program and had students from the business school, the law school, and the school of informatics and computing in the class together.) We're connected to the network in everything that we do, so having an understanding of how things actually work in a networked environment becomes important. When you're looking at issues with Russia attacking network resources, if you have a technical understanding of what routing across an entire network means, and how you acquire assets in that network and how it's actually working, it informs how you think about policy. I think a course would be more beneficial where you may not have to build out a network application, but you learn how those protocols work and what the vulnerabilities are in those protocols. If you have that level of technical knowledge, it helps you to assess policies and helps you to understand what else needs to be considered, because you understand how these things are working. Programming helps with your algorithmic thinking. If you're gonna go to the technical level of trying to understand malware exploits, then the programming class becomes important. But overall systems, understanding how systems work, is very key to cyber policy, because everything we do today is being done on a networked system.
- My last programming class was HTML1, but I know more about the technical specifics of attacks than most random computer scientists I meet who don't study security. So what that means is, that if your students go into the wrong intro class, they might learn bad things about security in some of those entry-level computer science classes. Unless it is a class that is, for sure, offering insightful network security points, taking external courses on introduction to security and watching talks from technical conferences might offer an easier pathway for people who want to be policymakers. Computer languages change every five minutes. The attacks change every five minutes. I think the currency of your knowledge, understanding how things connect to each other, what kinds of vulnerabilities you face in an evolutionary way across the system, and how you destroy systems, with an eye on the purpose of the system, is essential. You're gonna have a different set of dominant vulnerabilities, from a policy standpoint, if you're looking at financial services, than if you are looking at, say, electrical grids. Learning that context as it intersects with those technical points of vulnerability, there's some art to that.

- Primary maintainer[s] of systems [need] to be aware of evolutions in legal and policy approaches that impact their day to day management, particularly if they're dealing with sensitive systems like financial services. And so those day to day maintainers do need to be aware of the basics of securities regulation: duties of oversight, FINRA, and all of that.

Curriculum Drivers

Focus group participants cited unique combinations of drivers impacting curriculum development:

- Educational landscape review
- Industry landscape review
  - The discussion on cybersecurity policy issues is of keen importance to us. Our preference is to reference the issues that evolve out of the cyber enterprise and related security issues, hence breaking the word 'cybersecurity' into two parts: "cyber" and "security."
- Available faculty expertise
  - The Hewlett-funded eCasebook Cyber Security Law Policy and Institutions[43] (free and available to the public) reflects years of thinking on my part about how you might create a typology and framework, a roadmap of concepts that integrate cybersecurity policy and law into a very systematic theory of how it all fits together.
  - We've left to individual faculty for a particular course to define the knowledge map of what would go into a class. As in all curricular plans, there's definitely an element of practicality: who is available to teach this semester.
  - You have a different institutional commitment signaled based on whether it's a permanent faculty member who is a full professor teaching courses, versus a different person, with potentially minimal actual policy-making experience, every semester.
  - When I think about the degrees, there is national security and law focused (UT Austin), cyber risk management (Boston), and tech-informed internationally focused (Tufts), and I think of them as all within the grand rubric of cyber security policy. It's a sufficiently broad area that it seems not unreasonable to have these different foci, partially by which school within the institution set it up and which faculty are present there.
  - What's done the most for us is the dual-degree program, which has given a pipeline of interested students a structure and a way to access courses in business and computer science that build off of one another in a way that they really couldn't otherwise. So, the curriculum was driven by the building blocks that we already had. And it depends on the faculty: we still have a dearth of faculty that we need to teach this.

[43] Robert Chesney, "Cyber Security Law, Policy, and Institutions (version 3.1)," *U of Texas Law, Public Law Research Paper No. 716* (August 23, 2021), https://ssrn.com/abstract=3547103.

- Cybersecurity industry and policy domain advisors
  - Our interest is “tech-informed cybersecurity policy with an international focus,” so we tried to find out what members of Congress wanted to know in cyber, and that formed the framework for our course ”Cyber for Future Policymakers.” It’s really bits and pieces of technology: quantum computing, how the web works, web protocols, identity management, cryptographic applications.
- NCAE-C Center for Academic Excellence designation
  - The CAE process is driving the next iteration of our curriculum. It’s forcing us to go to a cohort model which originally we were trying to shrink away from. It’s going to be a lot more regimented, especially on the technical side, and even to a degree on the business, and law sides as well. There’s going to be a lot more shoehorning than there used to be.
- 2017 ACM Joint Cybersecurity Curriculum
- NICE Workforce Framework data/Competency Areas
  - To make sure I was taking a comprehensive look at the policy skills students would need, I pulled out three competencies from NICE: Law, policy and ethics; Policy development; and Organization awareness.
  - I do think that the frameworks are especially weak when it comes to creating a typology of straight policy topics or legal topics, and they tend to lump all sorts of things together in loose ways that aren’t especially compelling. I don’t recognize them and they don’t look like the way I think about it at all.

Curriculum Currency and Future Directions

- That’s the thing that sucks about this field: you can’t leave anything alone for six months without it becoming covered in dust and cobwebs. It’s embarrassing.
- Unless you’re really doing research in the area, within a year or two, you’re completely out of date with the syllabus.
- Two years out of date and it looks like it was written in the Stone Age.
- We need to update our curricula to prepare our students for the jobs of the future, not the jobs of the past.
- We are looking to integrate technology (particularly AI) into the curricula in all disciplines on campus.
- We have a team working on big data and the issues that come up as we apply AI tools into the cyber enterprise, from pandemic health care, to ethnic and racial issues. What kind of management, ethics, policies, and laws need to be discussed, created, or done away with as advanced technologies impact humanity?

B. POLICY COURSE OFFERINGS

The following table represents the landscape of policy courses offered in the programs included in this study. We included classes that reference any facet of cyber policy, even when secondary to the course's primary focus.

The Knowledge Area column reflects the authors' best attempt to place the course within a primary CSEC2017 Cybersecurity Curriculum Knowledge Area. (See Appendix F for definitions.)

The Cyber column identifies whether, according to available course descriptions, the class content focuses on cybersecurity ("Yes"), includes cybersecurity as a secondary topic ("related"), or is not cybersecurity-specific ("No"). "Req" indicates whether the course is required or elective.

Course Title (with links in online version of this report)	Univ	School/Dept	Knowledge Area	Cyber	Req
TMGT K5126: Strategic Advocacy	C	Technology Management	Organizational	Related	Yes
TMGT PS5125: Technology and Law	C	Technology Management	Societal	Related	Yes
TMGT PS5140: Managing the Entertainment Technology Multiverse	C	Technology of Management	Societal	No	No
14-817: Cyber Risk Modeling	CMU (MSIS)	Information Networking Institute - College of Engineering	Organizational	Yes	No
14-782: Information Security Risk Management I	CMU (MSIS)	Information Networking Institute — College of Engineering	Organizational	Yes	No
14-788: Information Security Policy and Management	CMU (MSIS)	Information Networking Institute - College of Engineering	Organizational	Yes	No
95-760: Decision Making Under Uncertainty	CMU (MSISPM)	Information Systems and Public Policy	Organizational	No	Yes
95-744: Cybersecurity Policy and Governance I	CMU (MSISPM)	Information Systems and Public Policy	Organizational	Yes	Yes
95-743: Cybersecurity Policy and Governance II	CMU (MSISPM)	Information Systems and Public Policy	Organizational	Yes	Yes
ISS 6216: Foundations of Globalization	FIU	International and Public Affairs	Societal	No	Yes
ISS 5654: Foundations of Cybersecurity and Technology Policy	FIU	International and Public Affairs	Societal	Yes	Yes
LAW 7707: Cybersecurity and Privacy Law	FIU	International and Public Affairs	Societal	Yes	Yes
ISS 6655: Issues in Cybersecurity and Technology Policy	FIU	International and Public Affairs	Societal	Yes	Yes
ISS 6658: Cyber Warfare and Strategy	FIU	International and Public Affairs	Societal	Yes	Yes
AIT 701: Cyber Security: Emerging Threats and Countermeasures	GMU	Information Sciences and Technology Department	Societal	Yes	No

AIT 678: National Security Challenges	GMU	Information Sciences and Technology Department	Societal	Yes	No
AIT 665: Managing IT Programs in the Federal Sector	GMU	Information Sciences and Technology Department	Organizational	No	No
AIT 679: Law and Ethics of Big Data	GMU	Information Sciences and Technology Department	Societal	Related	No
INTA 6103: International Security	GT	International Affairs	Societal	Related	No
MGT 6727: Privacy for Professionals	GT	Business	Organizational	Yes	No
PUBP 6502: Information and Communications Technology Policy	GT	Public Policy	Organizational	No	No
PUBP 8823: Geopolitics of Cybersecurity	GT	Public Policy	Societal	Yes	No
PUBP 6266: Policy Practicum	GT	Public Policy	Societal	Related	No
CS 6725: Information Security Policies and Strategies	GT				
	Computer Science	Organizational	Yes	Yes	
PUBP 6501: Information Policy and Management	GT				
	Public Policy	Organizational	Related	No	
PUBP 8813: Public Policy for the Digital World	GT				
	Public Policy	Societal	Related	No	
INFO-I 525: Organization Informatics and Economics of Security	IU				
	Informatics, Computing, and Engineering	Organizational	Yes	No	
INFO-I 537: Legal and Social Informatics of Security	IU	Informatics, Computing, and Engineering	Organizational	Yes	No
BUKD-C 548: Managing Intellectual Property in Global Business	IU	Business	Organizational	Yes	No
BUKD-T 560: IT Risk Management	IU	Business	Organizational	Yes	No
BUKD-T 578: Cybersecurity Law and Policy	IU	Business	Societal	Yes	No
LAW-B 536: Health Privacy Law	IU	Law	Societal	Related	No
LAW-B 587: Information Security Law	IU	Law	Societal	Yes	No
LAW-B 655: Information Privacy & Security Management Practicum	IU	Law	Organizational	Yes	No
LAW-B 708: Information Privacy Law 1 - Constitutional Privacy Issues	IU	Law	Societal	Yes	No
LAW-B 728: Information Privacy Law 2	IU	Law	Organizational	Yes	No
LAW-B 738: Cybersecurity Law II	IU	Law	Societal	Yes	No
LAW-L 730: Seminar in Intellectual Property: Data Law & Policy	IU	Law	Organizational	No	No
695.623: Information Security and Privacy	JHU (MS)	Engineering	System	Yes	No
695.791: Information Assurance Architectures and Technologies	JHU (MS)	Engineering			
	Organizational	Yes	No		
695.601: Foundations of Information Assurance	JHU (MS)	Engineering	Organizational	Yes	Yes

Strategy I	JHU (MA)	International Studies	Societal	Related	Yes
Strategy II	JHU (MA)	International Studies	Societal	Related	Yes
Intelligence I	JHU (MA)	International Studies	Human	Related	Yes
Intelligence II	JHU (MA)	International Studies	Human	Related	Yes
Air Power and Strategy	JHU (MA)	International Studies	Societal	No	No
American Defense Policy	JHU (MA)	International Studies	Societal	No	No
Behavioral Sociology of Conflict	JHU (MA)	International Studies	Societal	No	No
Defense Analysis	JHU (MA)	International Studies	Societal	No	No
Diplomatic Disasters	JHU (MA)	International Studies	Societal	No	No
Disinformation	JHU (MA)	International Studies	Societal	Yes	No
Economic Sanctions and Statecraft	JHU (MA)	International Studies	Societal	No	No
Genocide and Mass Violence	JHU (MA)	International Studies	Societal	No	No
Illicit Finance	JHU (MA)	International Studies	Societal	No	No
Insurgency and Irregular Warfare	JHU (MA)	International Studies	Societal	No	No
International Bargaining and Negotiation	JHU (MA)	International Studies	Societal	No	No
Operations Analysis	JHU (MA)	International Studies	Societal	No	No
Psychology and Decision-making in Foreign Policy	JHU (MA)	International Studies	Societal	No	No
Technology and War	JHU (MA)	International Studies	Societal	Related	No
The Nature and Character of Cyber Conflict	JHU (MA)	International Studies	Societal	Yes	No
GSCC1-GC1005: Cyber Law	NYU	Professional Studies	Societal	Yes	Yes
GSCC1-GC1010: National & International Cyber Organizations	NYU	Professional Studies	Societal	Yes	Yes
GSCC1-GC1015: Cyberpower & Global Security	NYU	Professional Studies	Societal	Yes	Yes
GSCC1-GC2000: Terrorism, Technology, and the Internet	NYU	Professional Studies	Societal	Yes	No
GSCC1-GC2015: Organized Cybercrime	NYU	Professional Studies	Societal	Yes	No
GLOB1-GC2065: Transnational Crime	NYU	Professional Studies	Societal	Related	No
GLOB1-GC2080: Transnational Terrorism	NYU	Professional Studies	Societal	Related	No
GLOB1-GC2227: International Investigations and Forensic Evidence	NYU	Professional Studies	Data	Yes	No
GLOB1-GC2000: Transnational Security	NYU	Professional Studies	Societal	Yes	No
GSCC1-GC1000: Cybercriminology	NYU	Professional Studies	Societal	Yes	No
GLOB1-GC2520: Advanced Colloquium (Transnational Security)	NYU	Professional Studies	Societal	Yes	No
GLOB1-GC2521: Disinformation and Narrative Warfare	NYU	Professional Studies	Human	Yes	No
GLOB1-GC3064: Responding to Emergencies in the Global System	NYU	Professional Studies	Organizational	Related	No
GLOB1-GC2516: Advanced Data Analysis for Global Affairs	NYU	Professional Studies	Data	No	No
GLOB1-GC3035: Analytic Skills for Global Affairs	NYU	Professional Studies	Societal	No	No
GSCC1-GC2900: Great Powers Competition and US Grand Strategy in the Eastern Mediterranean	NYU	Professional Studies	Societal	Related	No

GLOB1-GC2047: The Future of War	NYU	Professional Studies	Societal	Related	No
GLOB1-GC2070: Intelligence and Counterintelligence	NYU	Professional Studies	Data	Related	No
GSCC1-GC2225: National Security and Emerging Tech	NYU	Professional Studies	Societal	Yes	No
GLOB1-GC2650: Global Risk	NYU	Professional Studies	Organizational	Yes	No
GLOB1-GC200: Espionage and Economic Power	NYU	Professional Studies	Societal	Yes	No
IST 432: Legal and Regulatory Environment of Information Science and Technology	PSU (BS)	Information Sciences and Technology	Societal	Yes	Yes
SRA 111: Introduction to Security and Risk Analysis	PSU (BS)	Information Sciences and Technology	Societal	Yes	Yes
SRA 221: Overview of Information Security	PSU (BS)	Information Sciences and Technology	System	Yes	Yes
SRA 211: Threat of Terrorism and Crime	PSU (BS)	Information Sciences and Technology	Societal	Yes	Yes
SRA 311: Risk Analysis in a Security Context	PSU (BS)	Information Sciences and Technology	Organizational	Yes	Yes
INTAF 502: Science, Technology, and International Policy	PSU (MEng)	International Affairs	Societal	Related	Yes
LPE 851: Foundations in Public Law	PSU (MEng)	Law	Societal	No	Yes
LPE 852: Foundations in Private Law	PSU (MEng)	Law	Human	No	Yes
LPE 853: Engineering, Law and Policy Systems	PSU (MEng)	Law	Societal	Related	Yes
ENGR 497: Datafied Cultures and Privacy Law	PSU (MEng)	Engineering	Societal	Related	No
ENGR 597: Engineers and Scientists Shaping Policy	PSU (MEng)	Engineering	Societal	No	No
CS 201 / DHP D291: Cyber for Future Policymakers	Tufts	Computer Science & Global Affairs - Diplomacy, History, and Policies	Societal	Yes	Yes
CS 183 / DHP P237: Privacy in the Digital Age	Tufts	Computer Science & Global Affairs - Diplomacy, History, and Policies	Societal	Yes	Yes
DHP P249: International Cyber Conflict: An Introduction to Power and Conflict in Cyberspace	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	Yes	Yes
DHP P236 / CS 182: Cyber in the Civilian Sector	Tufts	Computer Science & Global Affairs	Societal	Yes	Yes
CS 184 / ILO L235: Cyberlaw and Cyberpolicy					
	Tufts	Computer Science & Global Affairs - International Law and Organization	Societal	Yes	Yes
CS 150-X/DS 153-X/DHP-P264: AI: Algorithms, Ethics, Policy					
	Tufts	Computer Science & Global Affairs - Diplomacy, History, and Policies	Societal	Related	No

CS 155-X: Ethics in Computer Science and Technology	Tufts	Computer Science	Societal	Related	No
CS151-X: Computing in Developing Regions	Tufts	Computer Science	Societal	No	No
DHP P231: International Communication	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	No	No
DHP P233: International Security					
	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	Related	No
DHP P235: Technology and Public Policy	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	Yes	No
DHP P238: Technology, Development, and Regulation	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	Yes	No
DHP P240: Role of Force in International Politics	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	No	No
DHP P245: Crisis Management and Complex Emergencies	Tufts	Global Affairs - Diplomacy, History, and Policies	Organizational	Related	No
DHP D290: Cyber Risk Management	Tufts	Global Affairs - Diplomacy, History, and Policies	Organizational	Yes	No
EIB B242: Innovation Models for Building Inclusive Businesses	Tufts	Global Affairs - Economics and International Business	Societal	No	No
ILO L200: The International Legal Order	Tufts	Global Affairs - International Law and Organization	Societal	No	No
ILO L201: Public International Law	Tufts	Global Affairs - International Law and Organization	Societal	Related	No
ILO L220: International Organizations	Tufts	Global Affairs - International Law and Organization	Societal	Related	No
ILO L221: Actors in Global Governance	Tufts	Global Affairs - International Law and Organization	Societal	Related	No
ILO L230: International Business Transactions	Tufts	Global Affairs - International Law and Organization	Organizational	Related	No
ILO L240: Legal and Institutional Aspects of International Trade	Tufts	Global Affairs - International Law and Organization	Societal	No	No
DHP D286: From Authoritarian Regimes to Illiberal Democracies	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	No	No
DHP H204: Classics of International Relations	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	No	No
DHP P200: International Relations: Theory and Practice	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	No	No
DHP P205: National Security Decision Making: Theory and Practice	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	Related	No
DHP P217: Global Political Economy	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	No	No
DHP P244: Modern Terrorism and Counterterrorism	Tufts	Global Affairs - Diplomacy, History, and Policies	Societal	Yes	No

EIB B231: International Business Strategy and Operations	Tufts	Global Affairs - Economics and International Business	Organizational	Yes	No
EIB B232: Work and Employment Relations in the 21st Century	Tufts	Global Affairs - Economics and International Business	Organizational	No	No
EIB B252: Corporate Social Responsibility in the Age of Globalization	Tufts	Global Affairs - Economics and International Business	Organizational	No	No
CYBER 200: Beyond the Code: Cybersecurity in Context	Cal	Information	Societal	Yes	Yes
CYBER 220: Managing Cyber Risk	Cal	Information	Organizational	Yes	No
CYBER 242: New Domains of Competition: Cybersecurity and Public Policy	Cal	Information	Societal	Yes	No
Cybersecurity Law & Policy	UT	Law	Societal	Yes	Yes
Cybersecurity Risk Management	UT	Law	Organizational	Yes	No
Electronic Discovery and Digital Evidence	UT	Law	Societal	Yes	No
Internet and Telecommunication Regulation	UT	Law	Societal	Related	No
Law of the Intelligence Community	UT	Law	Societal	Yes	No
Privacy Law	UT	Law	Societal	Yes	No
Seminar: Surveillance, Liberty, and Privacy	UT	Law	Societal	Yes	No
The International Law of Cyber Conflict	UT	Law	Societal	Yes	No
Seminar: Internet Law and Policy	UT	Law	Societal	Related	No
Seminar: Intellectual Property and Technology Policy	UT	Law	Societal	Related	No
Cyber Incident Response	UT	Law	Organizational	Yes	No
Seminar: Propaganda, Deception & Manipulation in the Technology Era	UT	Law	Human	Yes	No
Technology Transactions	UT	Law	Societal	Related	No
INTLPOL 300A: International Policy Speaker Series	S	International Policy	N/A	No	Yes
INTLPOL 301A: Research Methods and Policy Applications I	S				
	International Policy	Data	No	Yes	
INTLPOL 302: The Global Economy	S	International Policy	Societal	No	Yes
INTLPOL 301B: Research Methods and Policy Applications II	S	International Policy	Data	No	Yes
INTLPOL 306: Foreign Policy Decision-Making in International Relations	S	International Policy	Societal	No	Yes
INTLPOL 307: Policy Problem-Solving in the Real World	S	International Policy	Societal	No	Yes
INTLPOL 321: Fundamentals of Cyber Policy and Security	S				
	International Policy	Societal	Yes	Yes	
CS 182: Ethics, Public Policy, and Technological Change	S	Computer Science	Societal	Related	Yes

INTLPOL 225: Technology Policy, Innovation, and Startup Ecosystems: Japan and Comparative Perspectives	S	International Policy	Organizational	Related	No
INTLPOL 260: DigiChina Newsroom: Explaining Chinese Tech Policy	S	International Policy	Societal	Related	No
INTLPOL 323: Free Speech, Democracy and the Internet	S	International Policy	Societal	Related	No
INTLPOL 363: Confronting Misinformation Online: Law and Policy	S	International Policy	Societal	Yes	No
INTLPOL 276: Energy Markets and Policy	S	International Policy	N/A	No	Yes
CSCI 1860: Cybersecurity Law and Policy	Brown	Computer Science	Organizational	Yes	Yes
CSCI 1800: Cybersecurity and International Relations	Brown	Computer Science	Organizational	Yes	No
CSCI 1805: Computers, Freedom and Privacy	Brown	Computer Science	Societal	Yes	No
CSCI 1870: Cybersecurity Ethics	Brown	Computer Science	Human	Yes	No
CSCI 2002: Privacy and Personal Data Protection	Brown	Computer Science	Data	Yes	No
CSCI 1952X: Contemporary Digital Policy and Politics	Brown	Computer Science	Societal	Related	No

C. SYLLABI

Syllabi accessed during the course of research are listed below and hyperlinked in the online version of this report:

Brown

CSCI 1800 Cybersecurity and International Relations

CS1660: Computer Systems Security

CSCI 1310: Fundamentals of Computer Systems

CSCI 1330 Computer Systems

CSCI 1650: Software Security and Exploitation

Carnegie Mellon

14-642 - Introduction to Embedded Systems (MSIS)

15-605 - Operating System Design and Implementation (MSIS)

15-746/18-746 - Storage Systems (MSIS)

14-828: Browser Security (MSIS)

14-782: Information Security Risk Management I (MSIS)

95-760 Decision Making Under Uncertainty (MSISPM)

Introduction to Information Security Management (MSISPM)

Managing Disruptive Technologies (MSISPM)
Privacy in the Digital Age (MSISPM)
95-758 Network and Internet Security (MSISPM)

Georgia Tech

CS 6725: Information Security Policies
CS 6035: Introduction to Information Security
CS 6238: Secure Computer Systems
CS 6262: Network Security
CS 6250: Computer Networks

Indiana

INFO-I 520 - Security for Networked Systems
INFO-I 521 - Malware: Threat & Defense
BUKD-T 578: Cybersecurity Law and Policy
LAW-B 738: Cybersecurity Law II

Penn State

CYBER 262: Cyber-Defense Studio (BS)
CYBER 342W: Cyber Incident Handling and Response (BS)
CYBER 366: Malware Analytics (BS)
IST 432 Legal and Regulatory Environment of Information Science and Technology (BS)
IST 456 Information Security Management (BS)
CMPSC 443: Introduction to Computer and Network Security (MEng)
CSE 543: Computer Security (MEng)
CSE 544: System Security (MEng)

Stanford

CS 182: Ethics, Public Policy, and Technological Change
CS 251: Cryptocurrencies and Blockchain Technologies
CS 106A: Programming Methodology

Tufts

CS 184 / ILO L235: Cyberlaw and Cyberpolicy
DHP P249: International Cyber Conflict: An Introduction to Power and Conflict in Cyberspace
CS 183 / DHP P237: Privacy in the Digital Age
CS 201 / DHP D291: Cyber for Future Policymakers

CS 202 / DHP D292: How Systems Work
CS 203 / DHP D293: How Systems Fail
Workshop (4-days) for Social Science and Legal Scholars: Putting the Tech into Cybersecurity Policy

UC Berkeley

CYBER 289: Citizen Clinic
Beyond the Code: Cybersecurity in Context

UT Austin

eCasebook: Cybersecurity Law, Policy and Institutions
389T: Cybersecurity Law & Policy

D. PRIMARY AND SECONDARY COURSE TOPICS BY PROGRAM

The provided graphs depict the classification of classes offered in different programs (including electives, except where noted) based on the CSEC2017 Joint Task Force Cybersecurity Curricula. The primary topic assigned to each class represents its central theme, while the secondary topics highlight additional themes addressed within the course.[44] Unlike primary topics, where a single knowledge area was selected for each course, the number of secondary topics assigned per course varies based on course content.

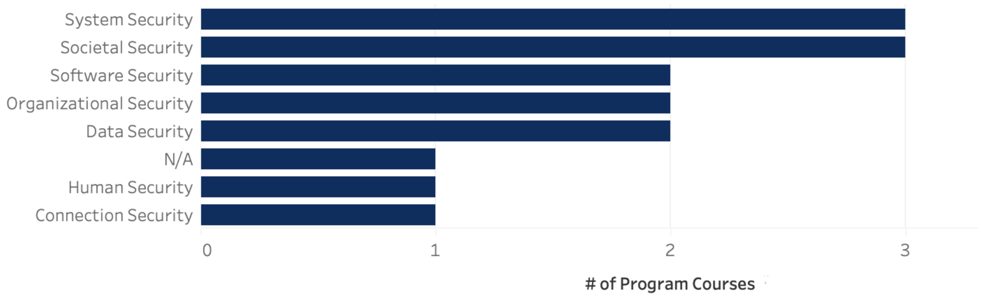
The knowledge areas we assigned for each course can be viewed in our aggregate data Excel spreadsheet.[45]

[44] It is important to note that these classifications are based solely on the course descriptions and available online information, which may introduce potential inaccuracies and limitations in the analysis process.

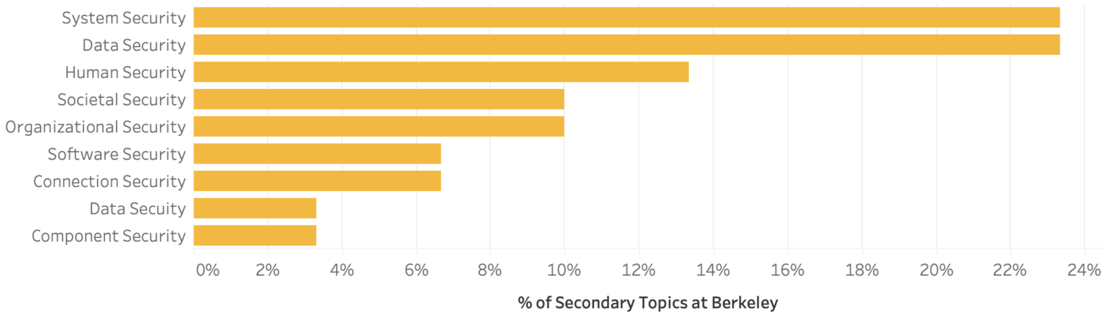
[45] https://docs.google.com/spreadsheets/d/12bbLAjoTloVxh8BcbHuAIdkMXTYbWaNpFgNrCM5Flwk/edit?usp=sharing

University of California, Berkeley

UC Berkeley - Primary Topics

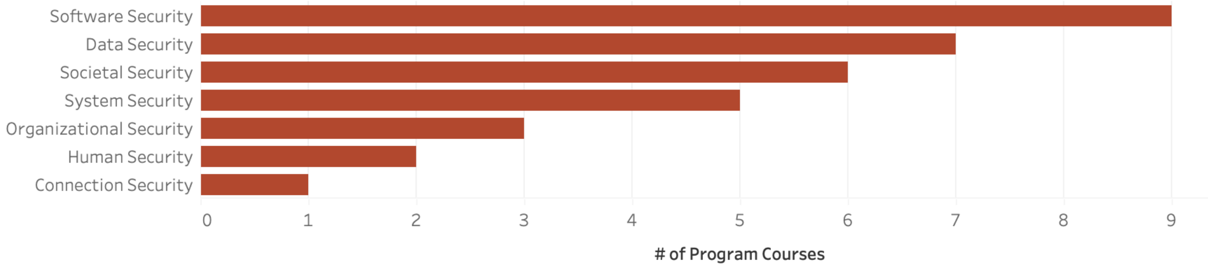


UC Berkeley - Secondary Topics

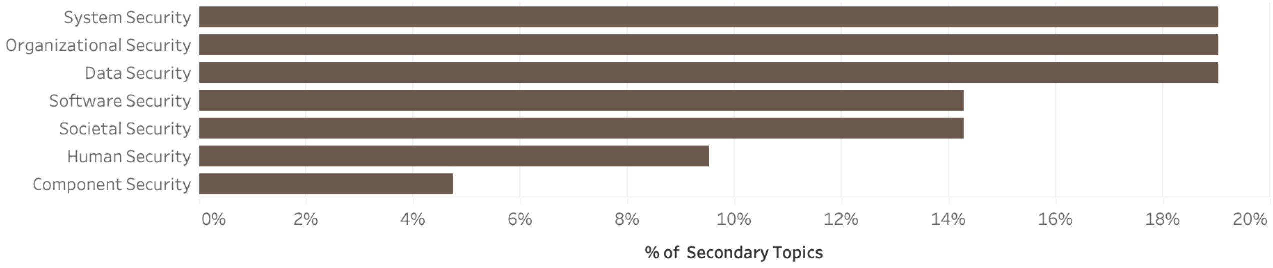


Brown University

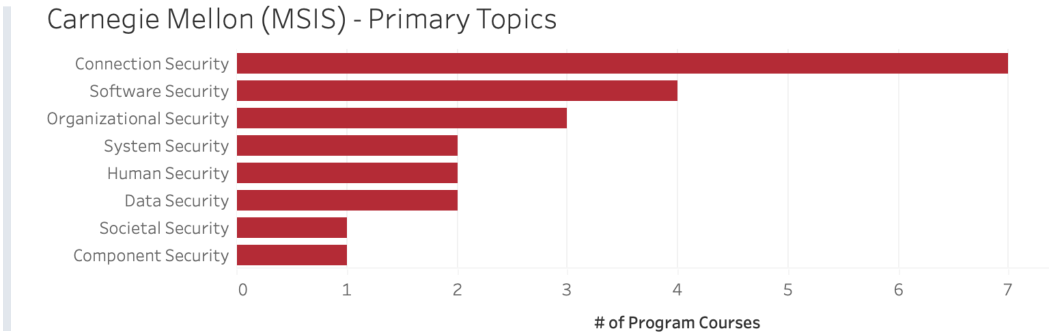
Brown - Primary Topics



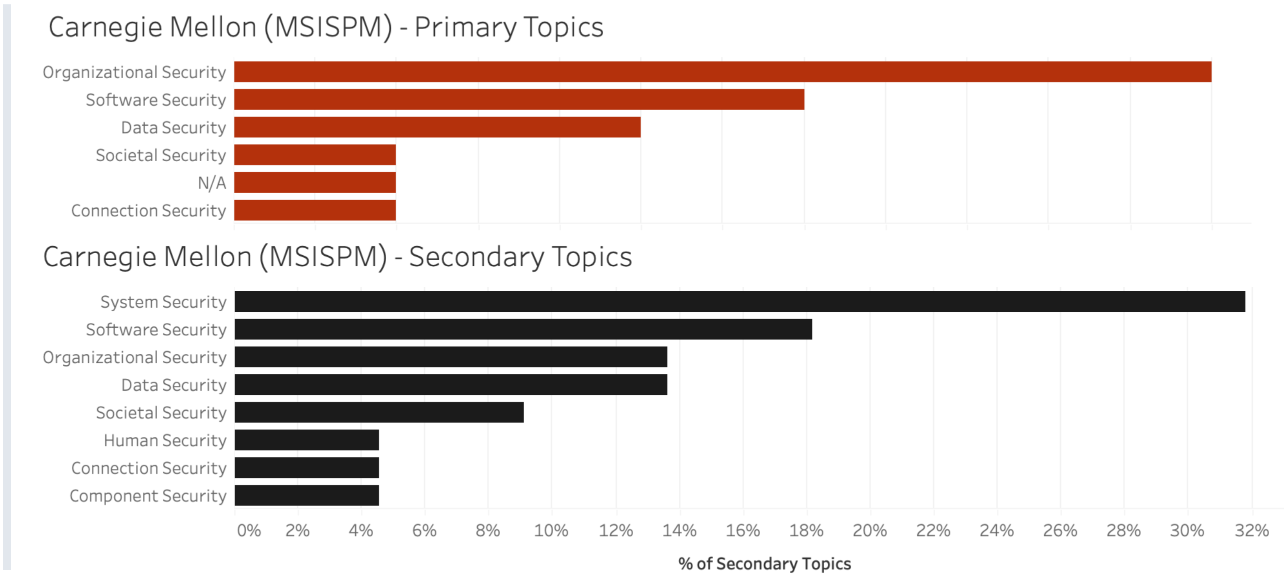
Brown - Secondary Topics



Carnegie Mellon University (MSIS) (not including electives)

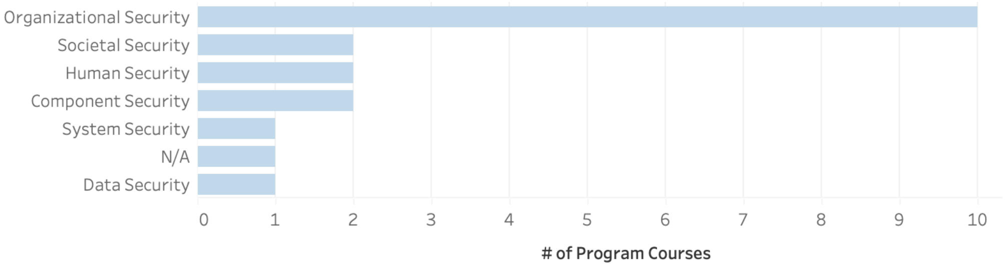


CMU (MSISPM) (not including electives)

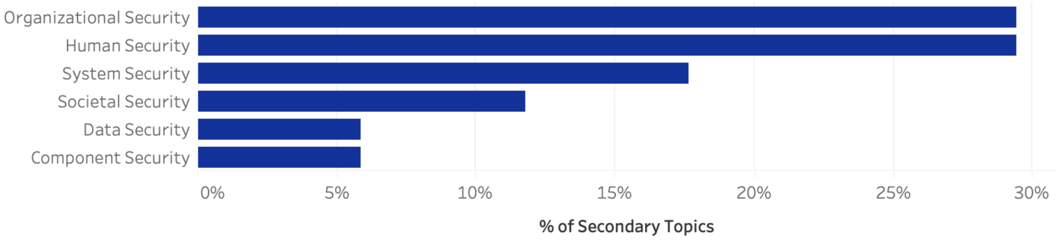


Columbia University

Columbia - Primary Topics

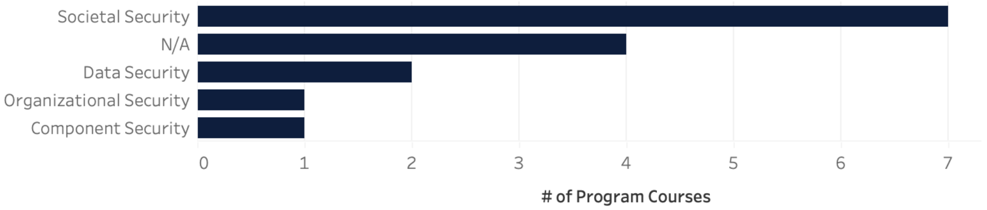


Columbia - Secondary Topics

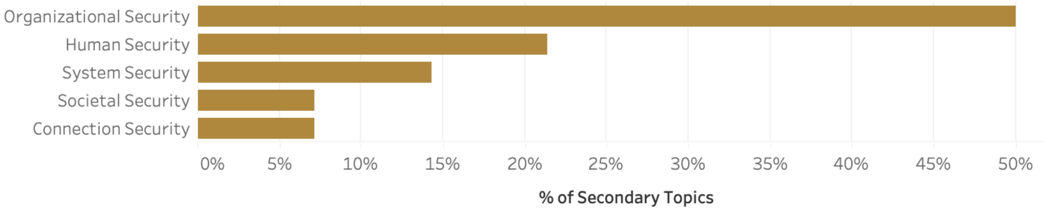


Florida International University

Florida International - Primary Topics

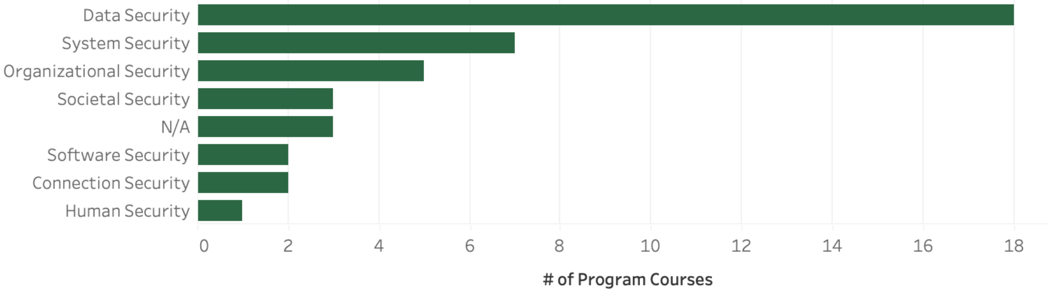


Florida International - Secondary Topics

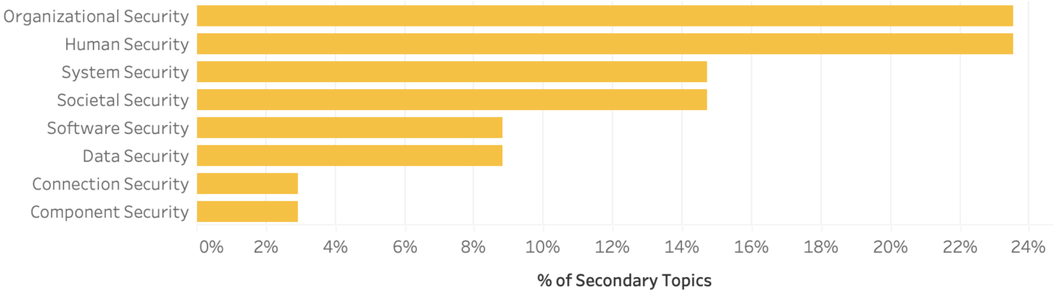


George Mason University

George Mason - Primary Topics

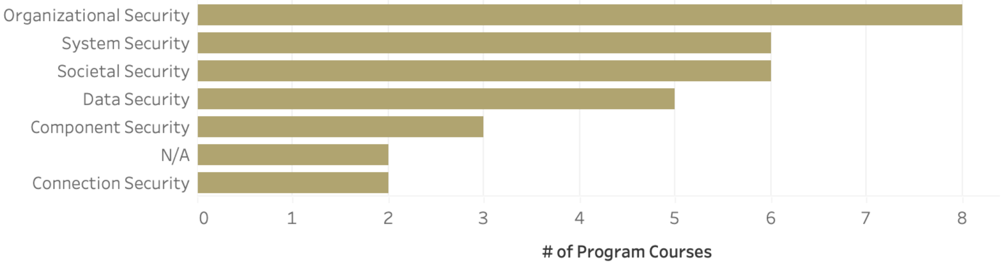


George Mason - Secondary Topics

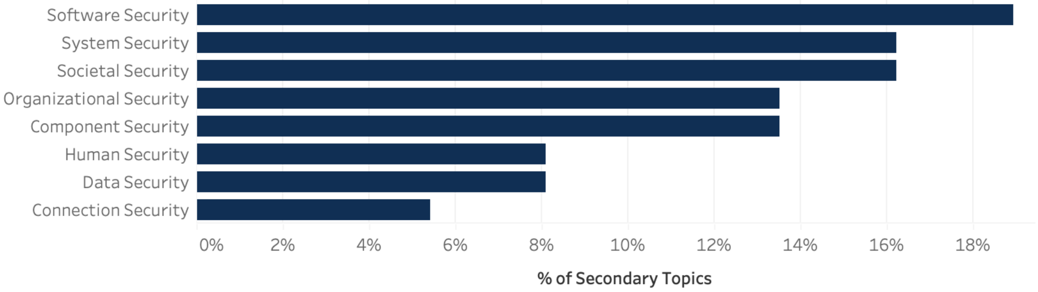


Georgia Institute of Technology

Georgia Tech - Primary Topics

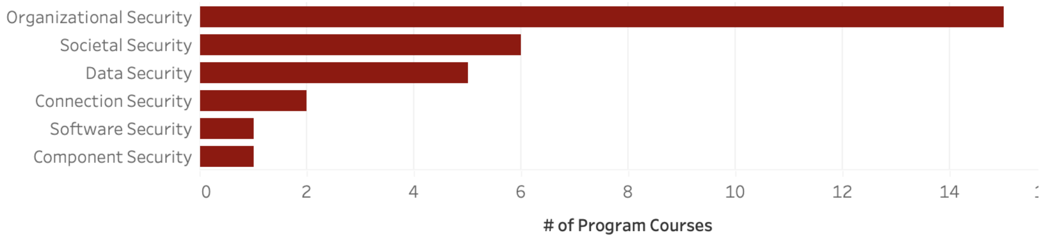


Georgia Tech - Secondary Topics

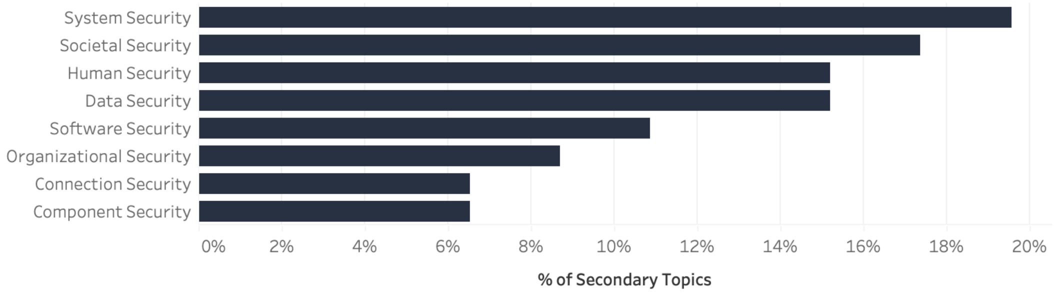


Indiana University (not including electives)

Indiana - Primary Topics

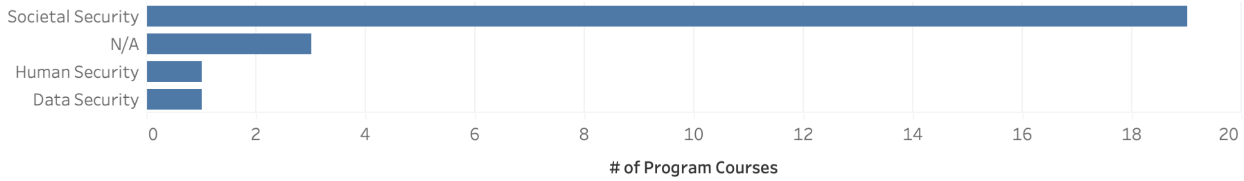


Indiana - Secondary Topics

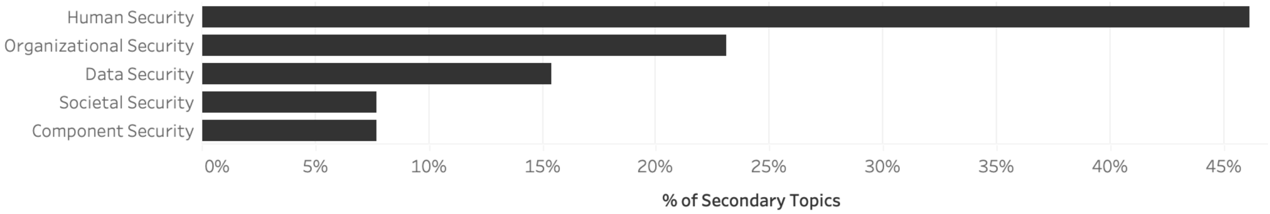


Johns Hopkins University (MA)

Johns Hopkins (MA) - Primary Topics

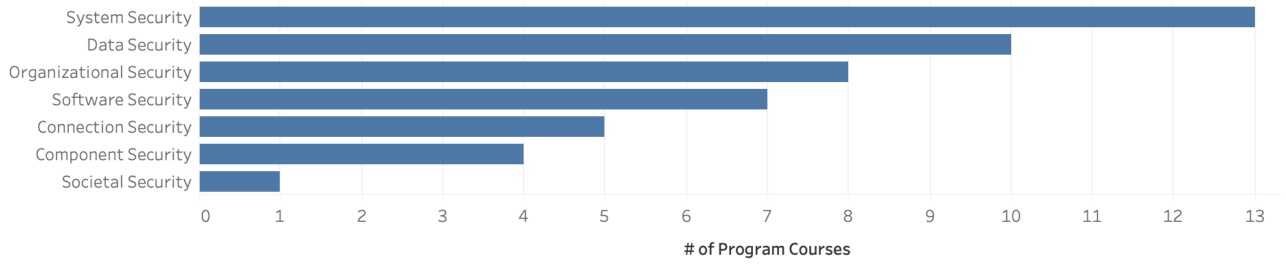


Johns Hopkins (MA) - Secondary Topics

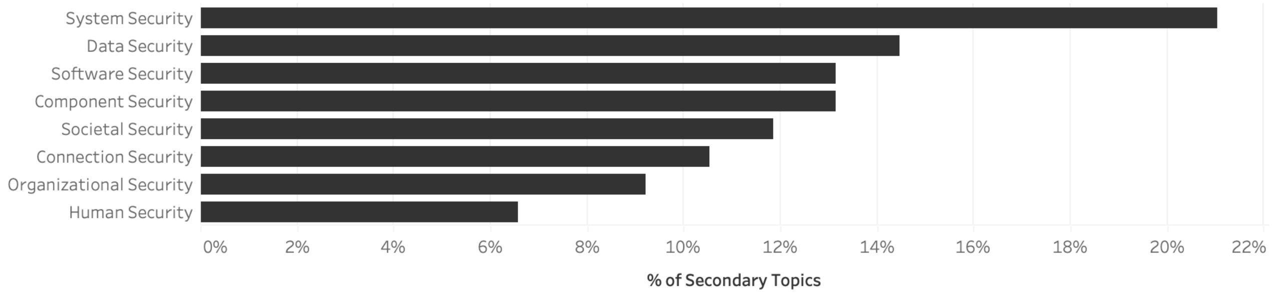


Johns Hopkins University (MS) (not including electives)

Johns Hopkins (MS) - Primary Topics

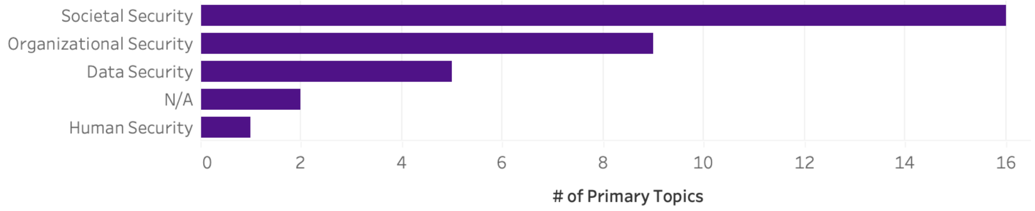


Johns Hopkins (MS) - Secondary Topics

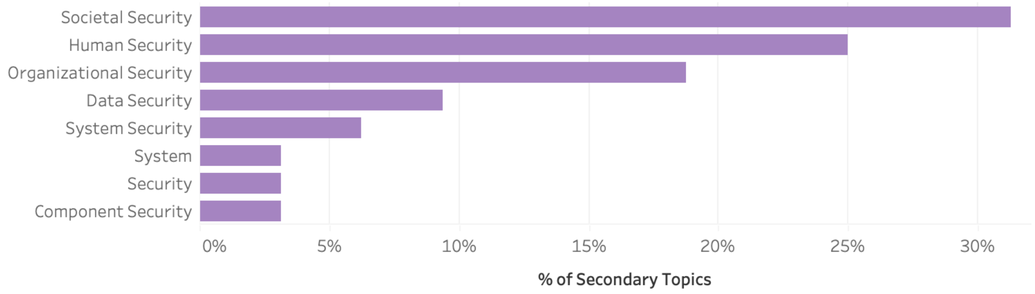


NYU

New York - Primary Topics

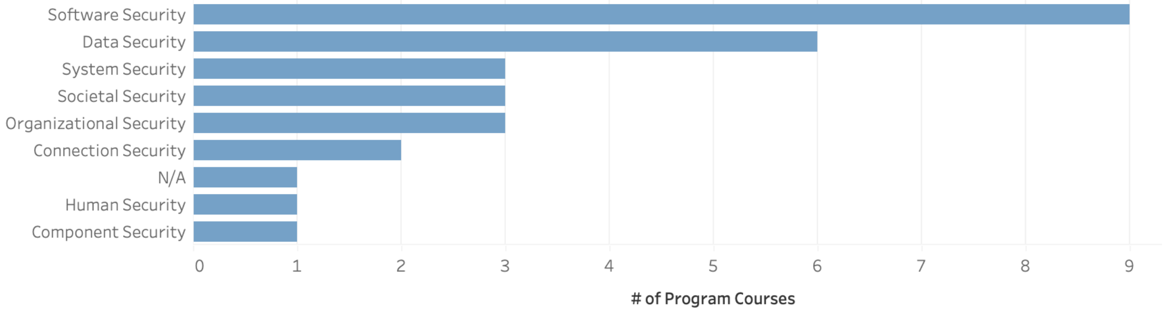


New York - Secondary Topics

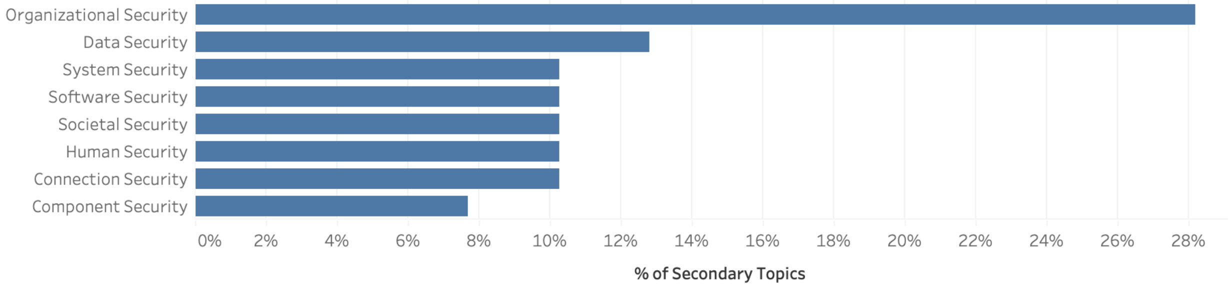


Pennsylvania State University (BS)

Penn State (BS) - Primary Topics

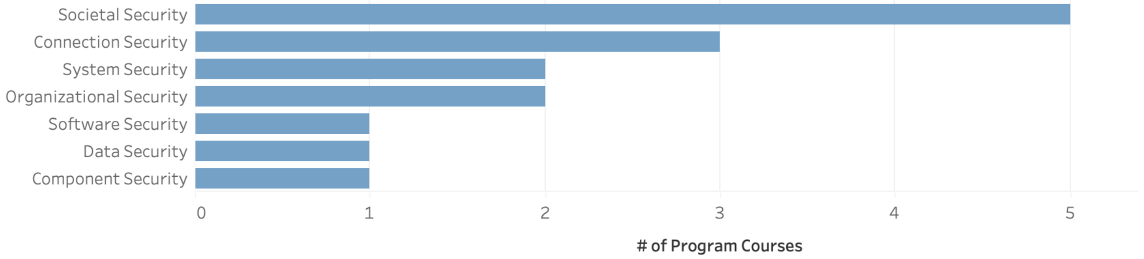


Penn State (BS) - Secondary Topics

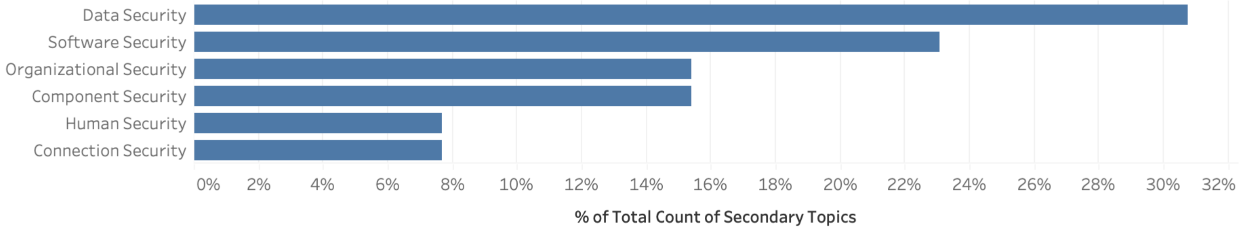


Pennsylvania State University (MEng) (not including electives)

Penn State (MEng) - Primary Topcis

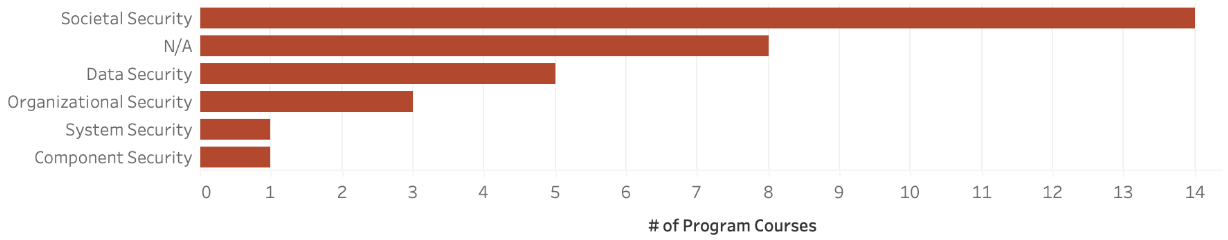


Penn State (MEng) - Secondary Topics

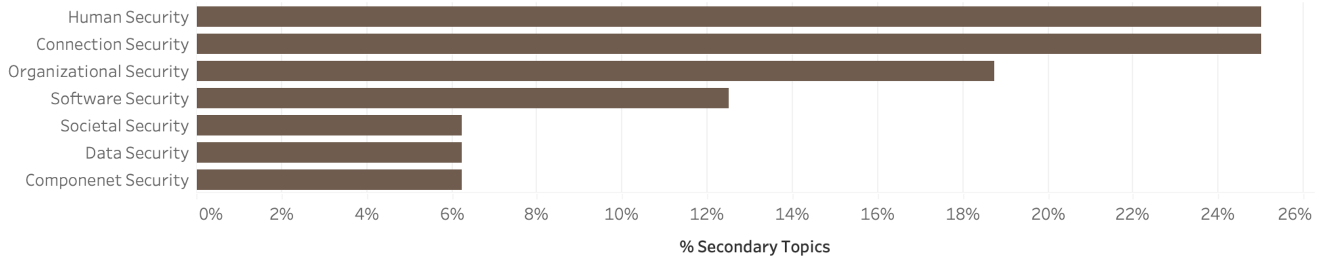


Stanford University (not including electives)

Stanford - Primary Topics

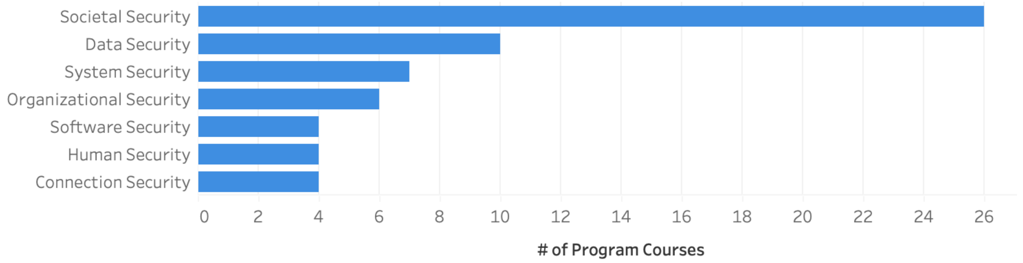


Stanford - Secondary Topics

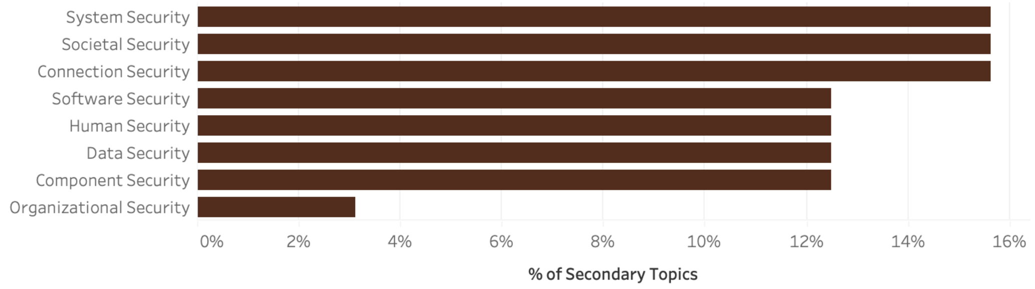


Tufts University

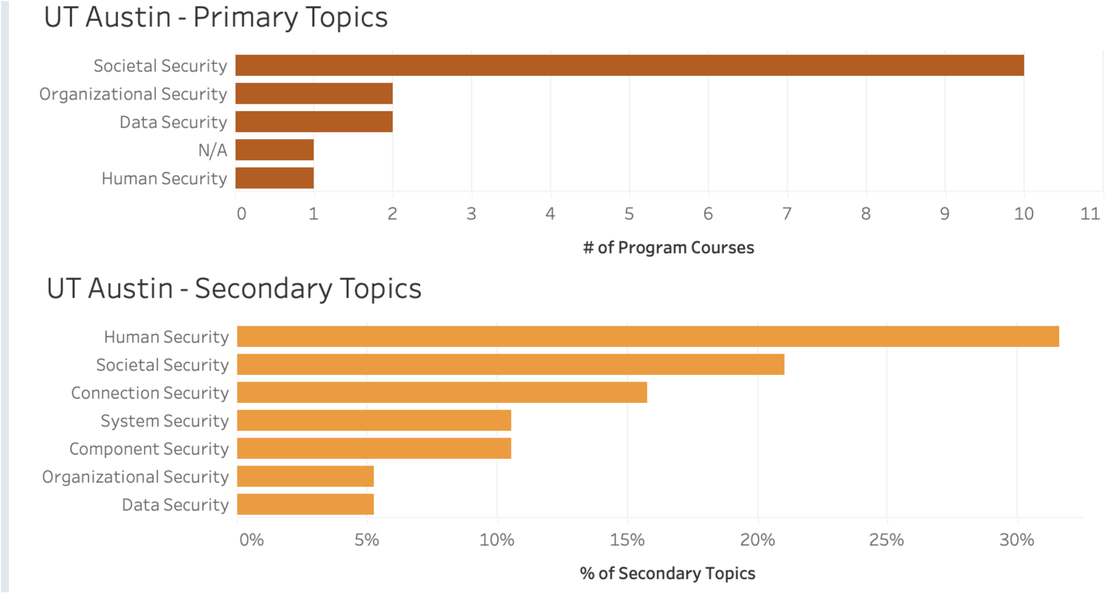
Tufts - Primary Topics



Tufts - Secondary Topics



University of Texas, Austin



UT Austin - Primary Topics

UT Austin - Secondary Topics

E. NICE FRAMEWORK SPECIALTY AREAS AND WORK ROLES

The following high-level outline of the National Initiative for Cybersecurity Education (NICE) Framework[46] is included as an alternate framing of interdisciplinary cybersecurity education. It provides a comprehensive taxonomy of knowledge, skills, abilities, and tasks associated with cybersecurity functions, specialty areas, and work roles. Use of the NICE Framework to describe and organize the work of the cybersecurity field is growing in education and training programs, for example through the National Centers of Academic Excellence in Cybersecurity (NCAEC) Program requirements.

The NICE knowledge requirement, "K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy," is ubiquitous throughout work roles in the NICE Framework. However, the framework concentrates policy tasks in the Specialty Areas of Strategic Planning and Policy[47] and Legal Advice and Advocacy[48] with less detail than the CSEC2017 framework selected for use in this study.

[46] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce- framework-cybersecurity-nice
[47] https://niccs.cisa.gov/workforce-development/nice-framework/work-roles/cyber-policy-and-strategy- planner
[48] https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/legal-advice-and- advocacy

SECURELY PROVISION (SP)

Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

1. Risk Management (RSK)
2. Software Development (DEV)
3. Systems Architecture (ARC)
4. Technology R&D (TRD)
5. Systems Requirements Planning (SRP)
6. Test and Evaluation (TST)
7. Systems Development (SYS)

OPERATE and MAINTAIN (OM)

Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

8. Data Administration (DTA)
9. Knowledge Management (KMG)
10. Customer Service and Technical Support (STS)
11. Network Services (NET)
12. Systems Administration (ADM)
13. Systems Analysis (ANA)

OVERSEE and GOVERN (OV)

Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.

14. Legal Advice and Advocacy (LGA)
15. Training, Education, and Awareness (TEA)
16. Cybersecurity Management (MGT)
17. Strategic Planning and Policy (SPP)
18. Executive Cyber Leadership (EXL)
19. Program/Project Management (PMA) and Acquisition

PROTECT and DEFEND (PR)

Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

20. Cybersecurity Defense Analysis (CDA)
21. Cybersecurity Defense Infrastructure Support (INF)
22. Incident Response (CIR)
23. Vulnerability Assessment and Management (VAM)

ANALYZE (AN)

Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

24. Threat Analysis (TWA)
25. Exploitation Analysis (EXP)
26. All-Source Analysis (ASA)
27. Targets (TGT)
28. Language Analysis (LNG)

COLLECT and OPERATE (CO)

Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

29. Collection Operations (CLO)
30. Cyber Operational Planning (OPL)
31. Cyber Operations (OPS)

INVESTIGATE (IN)

Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

32. Cyber Investigation (INV)
33. Digital Forensics (FOR)

F. CSEC2017 JOINT TASK FORCE CYBERSECURITY CURRICULA

The following knowledge area (KA) definitions, quoted from CSEC2017,[49] were used to categorize program coursework in this study:

Data Security

The Data Security knowledge area focuses on the protection of data at rest, during processing, and in transit. This knowledge area requires the application of mathematical and analytical algorithms to fully implement.

Software Security

The Software Security knowledge area focuses on the development and use of software that reliably preserves the security properties of the information and systems it protects. The security of a system and of the data it stores and manages , depends in large part on the security of its software. The security of software depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. The documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software. The Software Security knowledge area addresses these security issues. The knowledge units within this knowledge area are comprised of fundamental principles and practices.

Component Security

The Component Security knowledge area focuses on the design, procurement, testing, analysis, and maintenance of components integrated into larger systems. The security of a system depends , in part , on the security of its components. The security of a component depends on how it is designed, fabricated, procured, tested, connected to other components, used, and maintained. This knowledge area is primarily concerned with the security aspects of the design, fabrication, procurement, testing and analysis of components. Together with the Connection Security and System Security KAs, the Component Security KA addresses the security issues of connecting components and using them within larger systems.

Connection Security

The Connection Security knowledge area focuses on the security of the connections between components, including both physical and logical connections. It is critical that every cyberse-

[49] https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

curity professional have a basic knowledge of digital communications and networking. Connections are how components interact. Much of this material could be introduced through examples, and then abstracting to the essentials and introducing the appropriate vocabulary. Together with the Component Security and System Security KAs, the Connection Security KA addresses the security issues of connecting components and using them within larger systems.

System Security

The System Security knowledge area focuses on the security aspects of systems that are composed of components and connections, and use software. Understanding the security of a system requires viewing it not only as a set of components and connections, but also as a complete unit in and of itself. This requires a holistic view of the system. Together with the Component Security and Connection Security KAs, the System Security KA addresses the security issues of connecting components and using them within larger systems

Human Security

The Human Security knowledge area focuses on protecting individuals' data and privacy in the context of organizations (i.e., as employees) and personal life, in addition to the study of human behavior as it relates to cybersecurity.

Organizational Security

The Organizational Security knowledge area focuses on protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission. Organizations have responsibility to meet the needs of many constituencies and those needs must inform each of these knowledge units.

Societal Security

The Societal Security knowledge area focuses on aspects of cybersecurity that broadly impact society as a whole, for better or for worse. Cybercrime, law, ethics, policy, privacy and their relation to each other are the key concepts of this knowledge area. The threat of cybercrime across global society is incredibly serious and growing. Laws, ethics and policies are vital to the security of corporate and government secrets and assets, as well as to the protection of individual privacy and identity.

Policy Topics within CSEC2017 Knowledge Areas

Following is a curated list of policy topics culled from CSEC2017 Knowledge Areas:

- Societal Security
  - Cybercrime: Cybercriminal behavior, cyber terrorism, cybercriminal investigations, and economics of cybercrime;
  - Cyberlaw: constitutional foundation of cyber law, intellectual property related to cybersecurity, privacy laws, data security law, computer hacking laws, digital evidence, digital contracts, multinational conventions (accords), and cross-border privacy and data security laws;
  - Cyber Ethics: defining ethics, professional ethics and codes of conduct, ethics and equity/diversity, ethics and law, autonomy/robot ethics, ethics and conflict, ethical hacking, ethical frameworks, and normative theories;
  - Cyber Policy: international cyber policy, U.S. federal cyber policy, global impact, cybersecurity policy and national security, and new adjacencies to diplomacy;
  - Privacy: defining privacy, privacy rights, safeguarding privacy, privacy norms and attitudes, privacy breaches, and privacy in societies.

- Human Security
  - Social and Behavioral Privacy: social theories of privacy, social media privacy and security;
  - Personal Data Privacy and Security: sensitive personal data, personal tracking, and digital footprint;
  - Usable Security and Privacy: policy awareness and understanding, privacy policy.

- Organizational Security
  - Security Governance & Policy: privacy; laws, ethics, and compliance; security governance; managerial policy
  - Personnel Security: Special issue of privacy of employee personal information

- Data Security
  - Digital Forensics: legal Issues
  - Data Privacy

- Software Security
    - Ethics: Ethical issues in software development, social aspects of software development; legal aspects of software development; vulnerability disclosure; what, when, and why to test

The Component Security, Connection Security, and System Security knowledge areas do not include any significant coverage of policy topics.

VI. Acknowledgments

The authors extend special thanks to Ann Cleaveland, Executive Director, and Chuck Kapelke, Communications Specialist, from UC Berkeley's Center for Long-Term Cybersecurity for their expert guidance on this project and report.

We also wish to thank the William and Flora Hewlett Foundation for generously supporting this study and furthering the field of interdisciplinary cybersecurity education.

Thank you to the focus group members who added significantly to this report by sharing your insights on interdisciplinary cybersecurity education:

- Richard Aló – Florida A&M
- Bobby Chesney – University of Texas, Austin
- Chad Davis – Turtle Mountain Community College
- Kyle Eidahl – Florida A&M
- Andrew Grotto – Stanford University
- Dena Harito Tsamtis – Carnegie Mellon University
- Raquel Hill – Spelman College
- Susan Landau – Tufts University
- Andrea Matwyshyn – Penn State University
- Randy Pestana – Florida International University
- Scott Shackelford – Indiana University
- Fatemeh Shafiei – Spelman College

About the Authors

Lisa Ho is Academic Director of the Master of Information and Cybersecurity (MICS) program at the UC Berkeley School of Information. She oversees and manages curriculum and program design of the cybersecurity program, including the Citizen Clinic Public Interest Cybersecurity Practicum, and heads instructor hiring and development. Her prior roles included Campus Privacy Officer and IT Policy Manager with the Information Security and Policy team at UC Berkeley, and Technology Strategy Officer at San Francisco State University. She joined the higher education field with a background as system analyst in the technology and retail sectors. Lisa is also committed to multiple campus diversity, equity, inclusion, and anti-racism initiatives.

Sahar Rabiei is a graduate student in the Master of Cybersecurity and Information (MICS) Program at the UC Berkeley School of Information, and a recipient of the Curtis B. Smith Cybersecurity Fellowship. She currently serves as the MICS Cohort Representative. Sahar has held two distinct roles at the Center for Long-Term Cybersecurity: one focused on this project, and another involved the examination of corporate responsibility in cybersecurity and data ethics. She possesses a profound passion for the intersection of technology, policy, and cybersecurity, and is committed to bridging this intersection while pioneering innovative solutions for its intricate challenges.

Drake White is a full-time graduate student in the Master of Information Management and Systems (MIMS) program at the UC Berkeley School of Information. He holds a Bachelor of Science in Informatics from Indiana University. He is currently a part of the critical infrastructure Systems Research and Analysis team at Sandia National Labs, and is rigorously passionate about the public-good intersection of cybersecurity, ethics, policy, sustainability, and accessibility.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity | cltc.berkeley.edu | @CLTCBerkeley